agence d'évaluation de la recherche et de l'enseignement supérieur

Dossier d'évaluation
d'une unité de recherche

Vague E : campagne d'évaluation 2013-2014

Évaluation du

Laboratoire Spécification & Vérification (LSV – UMR 8643)

de l'École Normale Supérieure de Cachan

Table des matières

1 Présentation de l'unité 5
2 Réalisations 9
3 Implication de l'unité dans la formation par la recherche 19
4 Stratégie et perspectives scientifiques pour le futur contrat 20
5 Bilan récapitulatif 26
Annexe 1 : Présentation synthétique 27
Annexe 4 : Organigramme 31
Annexe 6 : Liste des publications 33
Annexe 7 : Liste des thèses 83

agence d'évaluation de la recherche et de l'enseignement supérieur

Dossier d'évaluation
d'une unité de recherche

Vague E : campagne d'évaluation 2013-2014

► Information sur l'unité de recherche

Nom de l'unité : Laboratoire Spécification & Vérification
Acronyme : L.S.V.
Nom du directeur pour le contrat en cours : Laurent FRIBOURG
Nom du directeur pour le contrat à venir : Laurent FRIBOURG

► Type de demande

Renouvellement à l'identique ☑ Restructuration ☐ Création ex nihilo ☐

► Choix de l'évaluation interdisciplinaire de l'unité de recherche

Oui ☐ Non ☑

Dossier d'évaluation

1 Présentation de l'unité

Fondé en 1997, le Laboratoire Spécification et Vérification (LSV) est le laboratoire d'informatique de l'ENS de Cachan, et est aussi affilié au Centre National de la Recherche Scientifique (CNRS) en tant qu'UMR 8643. La recherche au LSV est centrée sur la vérification de logiciels et systèmes critiques, et sur la vérification de la sécurité des systèmes informatiques. Il bénéficie du soutien de INRIA depuis 2002. Il compte aujourd'hui 24 membres permanents, 16 doctorants, 8 membres associés et 6 membres de support administratif et technique.

1.1 Politique scientifique

Le LSV consacre l'essentiel de ses recherches aux problèmes de la spécification et de la vérification des systèmes critiques. Il s'agit de développer des langages et des méthodes formelles permettant d'énoncer et de démontrer la correction de ces systèmes. Ces méthodes conduisent parfois au développement d'outils logiciels utilisés pour automatiser les preuves de correction ou, a contrario, la détection d'erreurs.

1.2 Profil d'activités

Le laboratoire est organisé en cinq axes, correspondant à cinq grands domaines d'application de nos techniques.

1. Axe DAHU : spécification et vérification des systèmes qui, tels les services web, reposent sur la manipulation de grandes bases de données distribuées. Membres permanents : Serge Abiteboul, Cristina Sirangelo, Luc Segoufin (responsable).
2. Axe INFINI : vérification automatique des systèmes infinis (programmes manipulant des données non bornées, processus communicant de façon mutuellement récursive, systèmes paramétrés, etc.). Membres permanents : Stéphane Demri, Laurent Doyen, Alain Finkel (responsable), Sylvain Schmitz, Philippe Schnoebelen.
3. Axe MEXICO : vérification des systèmes distribués et concurrents. Membres permanents : Benedikt Bollig, Thomas Chatain, Paul Gastin, Stefan Haar (responsable), Serge Haddad, Stefan Schwoon.
4. Axe SECSI : sécurité des systèmes d'information, allant de la vérification de protocoles de sécurité à la détection d'intrusions. Membres permanents : David Baelde, Hubert Comon-Lundh, Stéphanie Delaune, Jean Goubault-Larrecq (responsable).
5. Axe TEMPO : vérification des systèmes temps-réel, où la prise en compte des aspects temporisés est essentielle pour énoncer la correction. Membres permanents : Dietmar Berwanger, Patricia Bouyer-Decitre, Laurent Fribourg, Nicolas Markey (responsable), Claudine Picaronny.

Les axes DAHU, MEXICO et SECSI sont des projets de INRIA Saclay – Île-de-France.

Depuis novembre 2006, le LSV est membre de l'institut Farman, qui regroupe cinq laboratoires de l'ENS Cachan autour de la modélisation, la simulation, et la vérification des systèmes complexes.

1.3 Organisation et vie de l'unité

- **Evolution des effectifs.** Depuis 2008, les effectifs en chercheurs et enseignants-chercheurs ont légèrement augmenté passant de 21 en 2008 à 24 en 2013. Précisément, ceux qui ont rejoint le LSV sont : S. Abiteboul (DR INRIA), D. Berwanger (CR CNRS), S. Schmitz (MC ENS Cachan) et C. Sirangelo (MC ENS Cachan) en 2008 ; L. Doyen (CR CNRS) et S. Schwoon (MC ENS Cachan – Chaire INRIA) en 2009 ; D. Baelde (MC ENS Cachan) en 2012. Ceux qui ont quitté le LSV sont : F. Jacquemard (CR INRIA) et S. Kremer (CR INRIA) en 2011, G. Steel (CR INRIA) en 2012 ; É. Lozes (MC ENS Cachan) en détachement en Allemagne depuis 2010 (souhaite revenir en France sur un poste de professeur hors ENS Cachan).
- **Thèses soutenues.** Durant la période janvier 2008 – juin 2013, 28 thèses de doctorat (3 en 2008, 5 en 2009, 6 en 2010, 7 en 2011, 5 en 2012, 2 entre janvier et juin 2013) et 8 HDR (1 en 2009, 5 en 2011, 2 en 2012) ont été soutenues au LSV. Sur les 28 personnes ayant soutenu une thèse, 6 ont aujourd'hui un poste de MC (4 en France, 1 en Roumanie, 1 en Inde), 1 a un poste de CR CNRS, 8 sont en post-doc à l'étranger, les autres sont professeurs en classes spéciales, ingénieurs ou experts techniques dans des ministères.

  Notons que par année, nous avons en moyenne 18 doctorants inscrits pour 15 HDR, ce qui correspond à un peu plus d'un doctorant par HDR. Ce chiffre peut paraître faible. Nous aurions sans doute la capacité d'encadrer davantage de doctorants. Il est en partie compensé par un taux remarquable d'accession de nos étudiants à la vie universitaire et académique.
- **Liens avec INRIA.** Alors que seul l'axe SECSI correspondait à une Équipe-Projet Commune (EPC) avec l'INRIA en décembre 2007, deux autres axes EPC ont été créés en 2008 et 2009, à savoir DAHU et MEXICO. La création de l'axe DAHU a été renforcé par l'arrivée de Serge Abiteboul en décembre 2008 et le flux important des post-docs et chercheurs invités associés à son projet ERC Webdam ; l'axe MEXICO a correspondu à une restructuration de l'axe TEMPO qui s'est recentré sur sa composante « temporisée », après le passage de sa composante « systèmes distribués » dans MEXICO. La constitution de trois axes du LSV sur cinq en tant qu'EPC a naturellement renforcé la collaboration avec INRIA. Les trois EPC ont ainsi un processus d'évaluation quadri-annuelle par INRIA (dernière en date : 2010 pour MEXICO, 2011 pour SECSI, 2011 pour DAHU). La négociation de la contractualisation d'INRIA comme troisième co-tutelle du LSV (en sus de l'ENS Cachan et du CNRS) a débuté en 2012, mais n'a pas encore abouti pour des raisons essentiellement de calendrier.

- **Vie intérieure.** Le LSV a maintenu sa façon d'organiser sa vie intérieure qui a assuré depuis sa création une forte cohésion et l'implication de tous ses membres dans les tâches d'intérêt collectif :
  - comité de direction hebdomadaire (mardi, 10h-11h) ouvert à tous (ITA, représentant des doctorants compris), où est évoquée l'actualité non seulement du laboratoire mais du département,
  - séminaire hebdomadaire (mardi, 11h-12h), donné par un intervenant extérieur, suivi par tous les membres du LSV ainsi que, régulièrement, plusieurs membres extérieurs,
  - séminaire annuel de trois jours (fin mai ou début juin) à Barbizon ou un endroit proche de Paris, où tout le laboratoire échange des informations scientifiques, techniques et administratives.

1.4 Faits marquants

On présente cinq résultats qui ont eu un impact scientifique ces cinq dernières années, ou nous paraissent être porteurs d'impact pour les cinq prochaines années.

1. **Analyse d'APIs de sécurité (CI-44).** L'API PKCS#11 est aujourd'hui l'interface standard de sécurité la plus utilisée dans l'industrie. Par des méthodes de reverse-engineering automatisé et de démonstration automatique, l'outil Tookan, développé au LSV, découvre des bugs de sécurité dans des dispositifs PKCS#11 commerciaux (cartes à puce, hardware security modules, tokens de sécurité), et a ainsi mis à jour plus d'une douzaine de nouvelles attaques. Ce travail a fait l'objet d'articles dans le New York Times, le Boston Globe, le Suddeutscher Zeitung.

2. **XML avec information incomplète (RI-66).** La structure des documents XML est beaucoup plus compliquée que celle des bases de données relationnelles. En particulier, la gestion d'information incomplète est beaucoup plus difficile. Ce travail donne une étude systématique de l'information incomplète dans les documents XML en visant à la rendre indépendante de l'application visée. Nous donnons des classes de description de l'information incomplète qui sont robustes et débouchent sur des solutions algorithmiques efficaces.

3. **Synthèse distribuée pour systèmes à communications asynchrones (RI-118).** On cherche ici à dériver automatiquement un programme pour un système dont toutes les exécutions satisfont une spécification donnée et ce, quelle que soit la façon dont l'environnement se comporte. Pour le problème de synthèse de systèmes *distribués*, on se donne en outre une description des communications possibles entre les différents processus du système, ainsi que des communications entre l'environnement et les processus. Le but est de synthétiser automatiquement un programme pour chaque processus du système. Comme l'ont montré Pnueli et Rosner en 1990, ce dernier problème est indécidable en général. Le travail présent porte sur des systèmes ayant un comportement asynchrone. Un nouveau modèle de communication par *signaux* est introduit : un signal correspond ici à une action commune à deux processus, mais contrôlée par un seul. On montre que, dans ce cadre, le problème de synthèse est décidable pour les systèmes dont le graphe de communication est fortement connexe.

4. **Robustesse des systèmes temporisés (CI-50).** Nous proposons une méthode de synthèse des stratégies *robustes* garantissant l'atteignabilité d'un état-cible pour les automates temporisés. Par *robuste*, nous voulons dire que l'atteignabilité est obtenue, même en présence de petites perturbations induites par l'environnement sur les valeurs nominales des délais des automates. La sémantique de l'automate perturbé par l'environnement est modélisée sous forme de jeu entre contrôleur et environnement. On montre que l'atteignabilité se ramène à l'existence d'une borne supérieure sur la valeur des perturbations pour laquelle la construction d'une stratégie gagnante est un problème EXPTIME-complet.

5. **Well-quasi-orderings et complexité (CI-126).** Ce travail montre que les well-quasi-orderings peuvent être utilisés non seulement pour montrer la terminaison d'algorithmes, mais aussi, pour établir des bornes supérieures de complexité. En particulier, des bornes supérieures de complexité optimales sont extraites des preuves de terminaison à base du lemme de Dickson, pour des programmes à compteurs et structures de données associées.

1.5 Rayonnement et attractivité académiques

En ce qui concerne le rayonnement et la participation à la vie scientifique, parmi les nombreux prix, distinctions, participations à des instances de pilotage et d'évaluation impliquant des membres du LSV sur la période 2008-2013, signalons :

- Serge Abiteboul : ERC Advanced Grant (2009-2013), Chaire au collège de France (2012), membre du Conseil National du Numérique (2012), de l'Académie des sciences (2011), de l'Academia Europea (2012), ACM Fellow (2012),
- Michel Bidoit : nommé Directeur du département INS2I du CNRS (2013),
- Patricia Bouyer : ERC Starting Grant (2012-2015), Presburger EATCS Award (2011), membre élue du CoNRS (2012-2015),
- Hubert Comon-Lundh : médaille d'argent CNRS (2008),
- Stéphane Demri : lauréat d'une bourse Marie Curie extra-européenne (2012-2014),
- Laurent Fribourg : membre élu du bureau du Sénat Académique du campus Paris-Saclay (2013),
- Jean Goubault-Larrecq : médaille d'argent CNRS (2011),
- Philippe Schnoebelen : membre élu du CoNRS (2008-2012).

Par ailleurs, sur la période 2008-2013, les membres du LSV ont été *Program Chairs* ou *Conference Chairs* de 15 conférences internationales, et membres de 22 comités d'évaluation AERES. Voir annexe « Rayonnements et distinctions » pour un panorama plus détaillé.

En ce qui concerne l'attractivité, mentionnons que le LSV a obtenu pour des chercheurs étrangers :

- une chaire INRIA/MC ENS Cachan attribuée à Stefan Schwoon (2009-2014),
- une chaire d'excellence RBUCE-UP (FP7 - Marie Curie) attribuée à Giuseppe Lipari (2012-2014),
- une chaire d'excellence DIGITEO attribuée à Pierre McKenzie (2013-2015).

1.6 Interactions avec l'environnement social, économique et culturel

- Participation à la diffusion de la culture scientifique et l'engagement vis-à-vis de problèmes socio-économiques :
  1. Serge Abiteboul : co-rédacteur du rapport de l'Académie des Sciences sur l'Enseignement de l'Informatique en France (mai 2013) ; rédacteur principal du rapport sur la neutralité d'Internet du Comité National du Numérique (2013) ; a donné au Collège de France un cours de très haut niveau montrant l'impact de la logique du 1er ordre sur le monde moderne (2012) ; a donné des dizaines d'interviews radiophoniques et journalistiques sur la période 2008-2013.
  2. Paul Gastin a donné plusieurs séminaires à destination des professeurs de lycée (terminales, classes préparatoires) à l'ENS Cachan (juin 2010) et au CIRM de Marseille (mai 2013) pour sensibiliser et former des professeurs suite à l'introduction de l'informatique en terminale scientifique et à la modification du programme de l'option informatique des classes préparatoires.
  3. Jean Goubault-Larrecq a participé à plusieurs journées de communication et diffusion du logiciel de détection d'intrusion ORCHIDS à destination des industriels (speed-dating *iMatch* organisé par INRIA Saclay en novembre 2010, journée INRIA Industrie en avril 2012, séminaire *DGA Innosciences* en juin 2013, . . .).
- Liste des brevets et contrats avec industriels :
  1. Certificat APP Tookan en 2011, et contrats INRIA avec Boeing en 2010, Barclays en 2010, HSBC en 2011 (CI-44).
  2. Contrat d'étude du LSV pour le cabinet AdviTech Partners en 2009 : étude de faisabilité de la startup SpidWare dans le domaine de la sécurité informatique.
  3. Projet blanc CPP (confiance, preuves et probabilités) en 2009-2013 avec LSV (coordinateur), CEA Saclay, INRIA, Supélec, Dassault Systèmes, Hispano-Suiza, Safran (ex. SagemCom).
  4. Certificat APP Orchids délivré en 2012, suivi d'une convention INRIA-DGA sur Orchids, 2013-2016.
  5. Contrat ANR VALMEM avec LSV (coordinateur), LIP6 et STMicroelectronics de 2007 à 2010 ; validation de la mémoire SPSMALL (RI-124).
  6. Contrat FARMAN entre LSV et EADS Astrium Space Technology, 2011-2012 (CI-38).

7. Accord CIFRE ENS Cachan-EADS : co-encadrement thèse Jean-Loup Carré (2007-2010) et participation au logiciel Penjili (propriétaire EADS) d'analyse statique de code C.
8. Contrats CIFRE avec EDF (thèse d'Arnaud Sangnier en 2008) et France Telecom/Orange (thèse de Camille Vacher en 2010).

Signalons enfin que le LSV, qui a recruté un ingénieur à plein temps à cet effet (2013-2014), joue un rôle moteur dans le développement et le déploiement de la plateforme CosyVerif, conçue en partenariat avec deux laboratoires parisiens (LIP6, LACL), et qui abrite plusieurs outils de modélisation et vérification implémentés au LSV (IMITATOR, CUNF, COSMOS).

2 Réalisations

2.1 Production scientifique

	2008	2009	2010	2011	2012	2013 jan.-juin	Total
ouvrages, chapitres, édition d'actes	7	20	5	12	4	4	52
revues internationales	22	23	40	16	34	12	147
invitations dans des conférences internationales	4	5	5	3	5	1	23
articles dans des conférences internationales	52	61	61	65	53	24	316
thèses de doctorat ou d'habilitation	4	6	6	12	7	2	37

Ce bilan appelle plusieurs remarques :

- Le bilan surpasse nettement et à tous les niveaux, celui de la période 2004-2008, alors que celui-ci était déjà remarquable.
- Cette information quantitative ne reflète pas l'excellence et la sélectivité des revues et conférences où paraissent ces publications (Information and Computation, Theoretical Computer Science, Logical Methods in Computer Science, J. Logic and Computation, SIAM J. of Computing, ACM Trans. on Computational Logic, J. Computer and System Sciences, Distributed Computing, ACM Trans. on Database and Systems, J. of Computer Security, Communications of the ACM, J. of the ACM, pour ne citer que quelques revues prestigieuses où sont parues nos publications en 2008-2013).
- Il n'y aurait pas beaucoup de sens à faire un bilan axe par axe, car de nombreuses publications sont co-signées par plusieurs membres d'axes différents.

Nous détaillons maintenant, axe par axe, le rapport scientifique de janvier 2008 à juin 2013[1].

2.2 Bilan scientifique

► Scientific report of axis dahu

The main goal of Dahu is to make database driven systems more reliable and more efficient. To achieve this we study problems such as specification and modelling of such systems, query evaluation and query optimization, verification. . .

During the evaluation period we have worked mainly on four objectives. The first one is tree automata theory, as those are implicit in many XML query languages and Schema languages. The second one is about distributed data management. The third one concerns the specification and verification of database driven systems. The last objective is about efficient evaluation of queries.

Objective 1 Tree automata theory

The links between models for XML and regular tree languages has been advocated in many places: Tree automata seem to be playing for semi-structured data and XML the role of the relational algebra for relational databases. As XML is central in our research, we have studied several models of tree automata with features that could be used for manipulating data. Not surprisingly, most of our results concern data words and data trees. Those are words and trees where each position contains a data value together with the classical label. Data trees can easily be seen as a model for XML data.

[1] Ces rapports sont en anglais car ils réutilisent des parties des rapports scientifiques écrits par les EPC pour INRIA.

We obtained results on register automata: These extend the classical model of finite automata with auxiliary registers storing data values for later comparison. We have shown that they are closely related with timed automata (CI-172) and obtained various decidability and expressiveness results on data words and data trees, linking them with various logical formalisms such as XPath. See for instance (RI-121, CI-225, CI-137, CI-198, CI-250).

We also studied automata with counters as several variants of this automata model were used successfully for showing decidability of the above-mentioned register automata. Results here concern decidability and complexity issues. See (CI-206, RI-90, CI-197).

We also studied the expressive power of subclasses of regular tree languages using algebraic methods. As an application we derived from one such result a precise information about the expressive power of the query language XPath. Some of the associated references are (CI-302, RI-95, CI-241, CI-187, RI-77, CI-173).

We have also considered models described by tree automata enriched with a test of isomorphism between subtrees. They can be used for testing monadic key constraints over XML documents. For these models, the main challenge is to establish the decidability of the non-emptiness of the language specified by a given automaton, this was achieved by different techniques in (RI-142, RI-138, CI-255, RI-61, CI-178).

Finally we have obtained results concerning the closure of tree automata languages under various kinds of rewriting systems. The goal here is to be able to characterize this closure (exactly or with approximations) using a decidable formalism. This approach is useful for the analysis of transformations formalisms for semi-structured data. It has been applied in particular to typechecking XQuery updates and verifying access control policies. Some associated references are (CI-291, CI-251, CI-186).

Objective 2 Distributed data management

The goal is to develop a formal model for Web data management that would open new horizons for the development of the Web in a well-principled way, enhancing its functionality, performance, and reliability. Specifically, the goal is to develop a universally accepted formal framework for describing complex and flexible interacting Web applications featuring notably data exchange, sharing, integration, querying and updating.

Major results were obtained on the following topics:

Distributed knowledge base. As a foundation for managing distribution (CI-62), we have proposed a model of a distributed knowledge base, that handles data and meta-data, as well as access control and localization, in a unique integrated setting. To support automatic reasoning on this knowledge base, we also introduced a novel rule-based language supporting the exchange of rules, namely Webdamlog. This work has been presented (CI-120) and demonstrated (CI-132) at major database conferences.

Probabilistic XML. Data from the Web are imprecise and uncertain. To manage this imprecision in a well-principled way, we have made significant advances in the field of probabilistic databases, and specifically, probabilistic XML. We have introduced new tractable probabilistic models for representing uncertain hierarchical information, and carried out in-depth studies of query evaluation, aggregation, and updates in various probabilistic XML models. See for instance (CI-195, RI-109).

Data exchange and Web incomplete information. We have addressed the problem of restructuring data exchanged between communicating applications on the Web. We have proposed and analyzed a new language to specify data restructuring rules (schema mappings). This language generalizes existing mapping dependencies, by allowing a more flexible specification mechanism (RI-57). The data restructuring process also naturally generates partial information. We have proposed a general model of XML incomplete information and have studied the main computational problems related to it, ranging from consistency of partial specification to query evaluation (RI-66, RI-101). We have also investigated the possibility of efficient query answering solutions in the presence of incomplete information. In particular we have studied an efficient evaluation strategy referred to as "naive", because it ignores data incompleteness. We have considered this procedure for queries over general data domains, with the objective of identifying suitable query fragments where naive evaluation works (CI-14).

Jorge. We also invested a lot of effort in a textbook (undergraduate and graduate level) on Web data management (nicknamed Jorge) published at Cambridge University Press (LI-4). See http://webdam.inria.fr/Jorge.

Objective 3 Specification and verification of database driven systems

This objective aims at making systems manipulating data safer and more reliable. This means providing suitable models together with a toolbox for helping in the design and implementation of such systems. These last years we have mainly worked on the modelling and the static analysis at various levels: query language and XML schema, access control policies and global specification of data-centric evolving systems.

Modelling and verification of data-centric systems. We have intensively studied the Active XML model, a high-level specification language tailored to data-intensive, distributed, dynamic Web services. Our first line of results concerns the verification of temporal properties of runs of Active XML systems, specified in a tree-pattern based temporal logic, Tree-LTL. Our second line of result is a comparison of the specification power of various workflow control mechanisms within the Active XML framework and beyond. For more details about this work see (CI-134, RI-104, CI-292)

We have also introduced a model of automata designed for modeling infinite runs of systems equipped with static relational databases. The automata model is equipped with finitely many registers for storing data values for later comparison. The transitions of the automata depends on a conjunctive query involving the database and the current values of the registers. Our main contribution is the proof that automated verification of temporal properties of systems modeled by such automata model can be carried out in PSpace. For more details, see (CI-139, CI-5).

Static analysis of query languages. XPath is arguably the most widely used XML query language as it is implemented in XSLT and XQuery and it is used as a constituent part of several specification and update languages. Hence in order to perform static analysis on a system manipulating XML data it is important to master the static analysis for XPath. In general, in the presence of data values, the satisfiability of XPath is undecidable. However we have shown that many important fragments can be decided. For more details, see for instance (CI-137, CI-198, CI-250, CI-225).

Static analysis of updates and access control policies. XQuery language has been extended to XQuery Update Facility (a W3C Recommendation of 2011) in order to provide convenient means of modifying XML documents. We proposed a model for these update primitives as parametrized rewriting rules and gave type inference algorithms for these rules, directly applicable to XML static typechecking and to the verification of XML access control policies. For more details, see (CI-186, CI-149, CI-232).

Objective 4 Enumeration of answers to a query

In many applications the output of a query may have a huge size and enumerating all the answers may already consume too many of the allowed resources. In this case it may be appropriate to first output a small subset of the answers and then, on demand, output a subsequent small numbers of answers and so on until all possible answers have been exhausted. To make this even more attractive it is preferable to be able to minimize the time necessary to output the first answers and, from a given set of answers, also minimize the time necessary to output the next set of answers—this second time interval is known as the *delay*. For this it might be interesting to compute adequate index structures. Recently, we have exhibited many scenarios (restrictions on the database) for which enumeration of first-order queries can be achieved in constant delay after a linear preprocessing. The relevant bibliography is (RI-56, CI-16).

► Scientific report of axis infini

Twenty-five years after its initial theoretical developments, the framework of *Well-structured transition systems* (WSTS), developed in an ample part by members of the INFINI axis, has become an invaluable tool in the verification of infinite-state systems. Such systems are endowed with a well quasi ordering (wqo) $\leq$ on their state space, which allows to obtain various decidability results.

The rate with which new WSTS models are defined and used is still not diminishing. The use and the study of wqo has been renewed in the last ten years.

Objective 1 Complete WSTS and WSTS Completions

One of the most useful decidable problems on WSTS for verification is *coverability*, because it allows to check safety properties: given states s and t, decide whether $s \geq s_1 \rightarrow^* t_1 \geq t$ for some s_1, t_1. This is decidable thanks to a now classical backward algorithm, that attempts to reach s backwards from the set of states that cover t. Nevertheless, forward procedures are felt to be more efficient than backward procedures in general: e.g., for lossy channel systems, although the backward procedure always terminates, only a (necessarily non-terminating) forward procedure is implemented in the TREX tool.We have derived similar generic algorithms that proceed *forward*: those algorithms compute instead the *cover* of s, i.e., the downward-closure of the reachability set from s (CI-262, CI-239, CI-123, IN-5, RI-29). This work draws from topological generalizations of wqos, and comprises two main contributions:

- We define a *complete WSTS* as a WSTS S whose well-ordering is also a continuous directed complete partial ordering. This allows us to design a conceptual procedure $\mathbf{Clover}_S$ that looks for a finite representation of the downward closure of the reachability set, i.e., of the cover. This clearly separates the fundamental ideas from the data structures used in implementing Karp-Miller-like algorithms. Our procedure also terminates in more cases than the (generalized) Karp-Miller procedure. We characterize the complete WSTS for which $\mathbf{Clover}_S$ terminates. These are the ones that have a (continuous) flattening with the same clover.
- Building on our theory of completions (CI-262), we characterize those WSTS whose completion is a complete WSTS in the sense above. They are exactly the ω^2-*WSTS*, i.e., those whose state space is an ω^2-wqo. All naturally occurring WSTS are in fact ω^2-WSTS. Despite the fact that $\mathbf{Clover}_S$ cannot terminate on all inputs, that S is an ω^2-WSTS will ensure *progress*, i.e., that every opportunity of accelerating a loop will eventually be taken by $\mathbf{Clover}_S$.

Objective 2 Algorithmic Theory of WQOs

Except in a few pioneering works, the computational costs of WSTS-based methods has not really been analyzed or even addressed until recently. The explanation behind this omission is that the computer science community was lacking concepts and results on the complexity of the most commonly used wqos, beginning with tuples of natural numbers and words ordered by embedding. This issue goes beyond WSTS and verification.

In the last five years, we developed a theoretical framework that allows to measure the complexity of algorithms (and problems) involving these wqos:

- Complexity upper bounds are obtained by careful computations in the ordinal-recursive hierarchies first considered in Recursion theory and in Proof Theory. Our work here has a strong combinatorial flavor (CI-126, CI-119). We managed to provide upper bounds for several classical WSTSs—in particular lossy channel systems (CI-119, CI-24) and monotonic counter machines (CI-126)—and for some richer systems like timed-arc nets (CI-56).
- Establishing complexity lower bounds requires new reduction techniques. Following on our early success with lossy channel systems, we developed coding techniques for simulating ordinal-recursive computations in WSTSs in a robust way, i.e., with encodings that are compatible with the wqo. The versatility of these techniques is high and we could use them to prove very high lower bounds for a variety of systems: reset nets (CI-176), lossy channels (CI-24), timed-arc nets (CI-56), priority channels (Ra-6), etc.
- In parallel, we introduced and analyzed Regular Post Embedding problems. These can be seen as abstract, hence more manageable, versions of systems with lossy channels (CI-167, CI-181, CI-51, CI-39, CI-24). This is an initial step towards our goal of developing a rich array of complete problems for ordinal-recursive complexity classes (see project).

Objective 3 Algorithmics of Counter Systems

Although the study of counter systems (aka register machines) dates back to the '60s, this line of research was mostly about the theory of computability, with Minsky machines being a prominent example of a minimalistic universal model of computation. Our take with counter systems is rather to study their algorithmics, which finds numerous applications, not only for the verification of counter systems themselves (which can be seen as a particular class of programs manipulating integer variables), but also for questions about various logical frameworks (data, spatial, interval, relevance, linear, etc.)

In this regard, WSTS theory offers generic algorithms for *monotone* counter systems, and the complexity analyses of Objective 2 apply. Nevertheless, these bounds are not always optimal, and they simply do not apply to non-monotone models like VAS with hierarchical zero-tests. A finer, and often difficult analysis, that takes the specifics of the model into account, is then required.

In the last five years, we have investigated the algorithmic complexity of counter systems along several tracks:

properties: we have considered large classes of "coverability-like" properties and established their EXPSPACE-completeness on Petri nets and vector addition systems (VAS) (CI-106, RI-2),

extensions: we have worked on VAS extensions, for instance branching VAS (CI-188, RI-44), affine nets (CI-27), or VAS with a single zero-test (CI-203, CI-108, CI-97, RI-13), or

restrictions: on the contrary, we have investigated restrictions on counter systems that lead to decidability and lower complexities, like reversal-boundedness (CI-282) or flatness (RI-65, CI-55), and

memory: we have considered the model-checking problem for logics with a *freeze* operator (CI-197, RI-90, RI-27).

Objective 4 Games

We study games for *synthesis*, where the objective is to automatically synthesize an implementation that realizes a given specification. The synthesis question naturally reduces to game solving. We developed a quantitative theory of design and synthesis that includes several aspects in the specification, such as resource consumption, stochastic behaviors, and partial observation. We proposed several extensions of games and automata and studied their expressiveness and complexity. The main results have been obtained in:

- **quantitative games**, where we solved algorithmic questions for games with combinations of classical (Boolean) winning condition and quantitative winning conditions; the main results settled the complexity of mean-payoff parity games in NP $\cap$coNP, and the complexity of multi-dimensional energy and mean-payoff games as being coNP-complete;
- **quantitative specifications**, where we developed quantitative languages that enjoy both positive closure properties as well as decidability, which makes them appealing to specification-based design with quantitative constraints such as energy consumption; the main result is the new class of mean-payoff automata expressions, and the decidability of all interesting verification problems for them;
- **stochastic and partial-observation games**, where we consider various combinations of stochasticity, partial-observation, and quantitative objectives in games on graphs, useful to get algorithmic solutions of the synthesis problem. The main results show that Markov decision process with mean-payoff parity objectives can be solved in polynomial time, we give the complete picture of tight memory and complexity bounds for qualitative objectives in Markov decision process with partial observation, and we present striking results about partial-observation stochastic games with reachability objectives, showing surprising non-elementary bounds on the memory needed to win, equivalence of decision problems for pure and randomized strategies, as well as unexpected connections of such games with counter systems.

► Scientific report of axis mexico

The goal of the MExICo research axis, which is at the same time also an INRIA project-team, is ***M**odeling and **Ex**ploitation of **I**nteraction and **Co**ncurrency*. Our work consists in developing, exploring and exploiting adequate mathematical models to capture interaction and concurrency, and to develop these theoretical tools and results into effective and efficient methodologies for designing, verifying and monitoring distributed systems.

The problems addressed by MExICo being transversal to many domains, our work involves several application fields; in particular, we currently participate in the EU FP7 Project UNIVERSELF on autonomous telecommunications networks, and the HYCON2 Network of Excellence on *Highly-complex and networked control systems*. Other topics include web service composition security.

Objective 1 Automata and Logics

While automata models can be considered the core of system modeling and semantics, extensions and networked compositions are necessary to address complex systems and tasks.

MExICo has introduced weighted versions of MSO and CTL, which generalize both the boolean logics and their probabilistic counterpart. The use of weights from semirings allows us to incorporate further types of quantities such as energies or rewards, in addition to durations or probabilities, into automata models, and their extensions to pebble automata. Our results include a probabilistic Kleene theorem and find applications in XML query evaluation, which involves navigation for trees. Other extensions of MSO developed by MExICo concern languages over infinite alphabets. We have obtained decidability of MSO model checking of pushdown automata with registers and, more generally, logical and automata-theoretic frameworks for data words.

For *recursive* concurrent systems, we have developed an adequately powerful framework (concurrent visibly pushdown automata) and specification language, and shown that satisfiability and model checking are decidable in doubly exponential time.

A method for distributed synthesis in a natural framework with asynchronously communicating processes has been developed by Nathalie Sznajder, Paul Gastin *et al.* These works show that the distributed synthesis problem is decidable under mild assumption on the communication architectures, and may open the way to a decidable theory of distributed synthesis.

Objective 2 Partial Order Semantics

Occurrence nets, and the underlying (labeled) event structures, are well known partial order models for the concurrent behavior of Petri nets, which is given in the form of partially ordered runs rather than a collection of interleavings. In MExICo, these models constitute important instruments for verification (in particular via the MOLE tool that interfaces e.g. with model checkers). We have also extended ioco-style conformance relations to this partial order framework, and are currently pursuing the development of a *testing* methodology to check conformance of a concurrent implementation with respect to partial order specifications.

On top of the partial order and conflict relations in event structure,s we have introduced the *reveals relation* between events in occurrence nets. Essentially, event a is said to reveal event b if in any maximal run that contains a, b must also occur, be it before, after, or concurrently with a, and even if a and b are not causally related. In our previous work, was for occurrence nets that represent. However, the upper bound was prohibitive for computing the relation in practice. We have shown the reveals relation to be decidable for unfoldings of safe Petri nets, and to be also computable on a given occurrence net via efficient algorithms. Extending this line of research, we have generalized (RI-1) the reveals

relation to express more general dependencies, involving more than two events, and we introduced the ERL logic to express these dependencies as boolean formulas. A synthesis problem arises naturally: given an ERL formula ϕ, is there a finite occurrence net N such that N describes exactly the dependencies between the events of N? We solve this problem with a synthesis method that requires only two synthesis rules. Building on the extended reveals relation, we have recently developed an effective (PSPACE) methodology for *weak* diagnosis of faults : our method allows to detect, from a partial observation of concurrent behavior, whether or not an unobservable *fault* transition inevitably occurs—in the past of the observations, their future, or without causal relation.

Contextual nets are an extension of Petri nets that faithfully models concurrent read accesses to shared resources: such reads are independent and concurrent. Moreover, the unfolding of a contextual net may be up to exponentially smaller than for its non-contextual version. Our work on the theoretical foundations, as well as appropriate data structures and algorithms, has shown the practical efficiency of this approach (which was far from obvious before), and has resulted in an efficient tool, CUNF. Recently, we have made further steps towards improving this approach by investigating merged processes, a data structure that handles choices more efficiently than unfoldings. The implementation of this approach is currently under way.

Objective 3 Timed Systems

In concurrent and composite systems, the real time behavior is of even greater importance than in sequential, centralized ones, but also harder to apprehend. MExICo participates in several research efforts in this area, in particular the ANR project IMPRO on implementability and robustness of real-time systems.

The interplay of concurrency and timing behavior is one of the major research interests of MExICo. We have studied in particular

1. the relations between networks of timed automata on the one hand and time Petri net on the other, giving a concurrency-preserving translation between these models;
2. conditions under which the components in a network of timed automata can evolve *without* sharing the clocks between components, i.e. without the need for one component to read those of another; and
3. a constructive equivalence of Event Clock Message Passing Automata, a model extending the Event Clock Automata of Alur *et al.*

Objective 4 Stochastic Systems

The uncertainty present in concurrent real-time systems often calls for a probabilistic treatment; in the following, we select two of our contributions, to highlight the relevance of probabilistic models in our work.

We have designed a logic HASL for stochastic systems that can express elaborated performance indices related to path behaviours, and developed a tool COSMOS for statistical model checking for HASL formulas over a stochastic Petri net with general distributions. In parallel, we have developed the first importance sampling method for rare events that still produces a confidence interval (rather than an estimated value), and integrated this method in COSMOS.

In joint work with LIAFA, we have solved most of the open problems concerning *product-form Petri nets*. We have provided a sound and complete set of rules to synthesise product form Petri nets, characterized the complexity class of standard problems (liveness, reachability and coverability), and proposed a large subclass of product form Petri nets for which the crucial normalising constant can be efficiently computed. This paper has obtained the outstanding paper award of the ATPN 2011 conference (CI-129).

Currently we are investigating diagnosis and opacity issues in stochastic networks, which are issues we intend to pursue in-depth in the future.

► Scientific report of axis secsi

The SECSI research axis, also an INRIA project-team, is concerned about *security of information systems*. The aim of the SECSI axis is to *develop logic-based verification techniques for security properties of computer systems and networks*. It concentrates on designing automated proof techniques to establish security properties of cryptographic protocols and implementations. It generally aims at applying logic to make our systems and networks more secure, in particular in the area of intrusion detection.

Objective 1 Symbolic verification of cryptographic protocols

In 2008, most security properties that one could check were *trace* properties (secrecy, authentication, typically). This left out many important properties which can only be specified through observational equivalence of processes: e.g., vote-privacy, receipt-freeness and coercion-resistance in e-voting, fairness in contract signing. We started to explore decision procedures for static equivalence first (security against passive adversaries, roughly) (CI-224, CI-245, RI-37, RI-43, RI-10), modulo a large class of equational theories; we have also obtained theory combination results (CI-208). We then moved to observational equivalence (active adversaries) (RI-94), obtaining NP decision procedures (CI-236). The particular challenge of e-voting protocols also spurred the exploration of refined criteria and algorithms for observational equivalence (CI-183, TH-5). On the latter topic, we also studied the question in the presence of so-called group equational theories (CI-54), or with replication (Ra-7). We have also obtained algorithms for the related notion of trace equivalence (CI-90, CI-71, CI-22). Those algorithms have been implemented in dedicated tools (e.g. AKISS and APTE[2]), or integrated in Bruno Blanchet's ProVerif tool. They have been tested on e-voting protocols and on several versions of the electronic passport protocol.

Another concern that was addressed in the SECSI axis is *composition*, i.e., typically, whether putting two secure protocols in parallel is still a secure system. (This is wrong in general.) We designed sufficient conditions that offer such guarantees, even when some long-term keys are shared between the protocols (RI-125, CI-184, CI-266), or when a user chooses the same password for different applications (CI-298, CI-81). This also led us to propose and prove sound some prudent engineering practices that are easily implementable

[2] http://projects.lsv.ens-cachan.fr/APTE/

by protocol designers. We have extended this to composition with sharing of secrets in (CI-52), in an observational equivalence setting, and we have applied it to the ICAO electronic passport standard.

We also addressed the question of producing formal security proofs in a proof assistant such as Coq, as is required more and more often. Instead of writing them by hand, which is tedious, one can instead have them produced automatically by an instrumented model-checker, as described in (CI-301, RI-70).

Objective 2 Computational models

The standard models of security in cryptography are *computational*: messages are actual bit strings, and adversaries and randomized polynomial time machines which communicate on shared tapes. Arguably, computational models are more *faithful* to actual implementations of cryptography than symbolic models (even with equational theories); but computational security proofs are less easily automated.

In this field, we have pursued the path of *computational soundness* theorems. Such theorems state that, under some assumptions, any protocol that is secure in a given symbolic model is also secure in a computational model: we obtain the best of both worlds. See (RI-91) for a state-of-the-art report on symbolic methods for obtaining computational proofs.

We have produced general frameworks (RI-120) for comparing symbolic and computational models. Contrarily to other work on the topic, the set of cryptographic primitives is not fixed, and is a tunable parameter (exclusive-or, ciphers, lists, symmetric encryption, modular exponentiation are examples); an extension is needed, and obtained, for bilinear pairings (RI-71). The soundness theorems we obtained apply to the cases of passive and adaptive adversaries.

The situation with *active* adversaries is more complex. Previous work only considered soundness results relying on trace mappings, which failed to account for indistinguishability (observable equivalence) properties. We have obtained the first computational soundness result for *observational equivalence* (CI-269). This had been an open problem for several years.

Objective 3 Applications (e-voting, security of APIs, circuits)

General verification techniques should be complemented with actual, specific applications. We have looked at a number of important classes of cryptographic protocols and implementations.

First and foremost, we have examined the hot question of verifying *e-voting* systems. The relevant security properties there are numerous, subtle, and hard to define formally and to verify (fairness, eligibility, vote privacy, individual and universal verifiability, coercion resistance, etc.). They justified a good deal of the research presented in previous subsections. We gave the first symbolic definitions for these properties, and analyzed several electronic voting protocols (Ch-11). Verifiability was dealt with in (CI-164), with applications to the FOO'92, Helios 2.0 and JCJ/Civitas protocols. Importantly, our approach highlights the exact parts of the voting system that need to be trusted in order to achieve the properties.

We have also looked at *cryptographic APIs*, such as RSA's PKCS#11, a widely used API used in hardware security modules (HSM) USB security tokens, and smartcards. We managed to overcome the problem of modeling mutable global state, previously identified as a barrier to such a project[3], and found several previously unknown attacks on the standard (CI-299). Further work led to results on proprietary variations (RI-69), and abstraction results permitting security proofs for unbounded fresh keys (CI-226). The model developed in this work is the basis of the Tookan tool[4], which reverse-engineers the configuration of the device under test, builds a model for a model checker, and executes any attack trace found by the model checker directly on the device. Testing on 18 commercially available devices led to the discovery of 10 previously unknown attacks (CI-151). Licenses were sold to Boeing, Barclays, HSBC. Related work included investigating the security of the YubiKey hardware device (CI-40). We also managed to make Bleichenbacher's "million message attack" practical on the RSA PKCS#1v1.5 standard for public key encryption, as used in TLS/SSL for example (CI-44). This led to widespread interest, as one can judge from articles in the New York Times, Boston Globe and Süddeutscher Zeitung.

Objective 4 Protection of hosts and networks

There is more to computer security than cryptographic protocols, APIs, and implementations. We have recognized (since 2001) that we could have some impact in other fields of computer security, and in particular in *intrusion detection*. Our intrusion detection tool ORCHIDS is based on a remarkably efficient, on-the-fly model-checking algorithm for detecting subsequences of events that satisfy some possibly complex

[3] Herzog, J., *Applying protocol analysis to security device interfaces*, IEEE Security & Privacy Magazine, 2006:4(4),pp. 84–87
[4] TOOl for cryptoKi ANalysis, `http://secgroup.ext.dsi.unive.it/tookan/`

formulae. See (IN-23), which explains the kind of mischievous attacks ORCHIDS is able to detect, explains the basic algorithm, several of the important optimizations, and gives a formal proof of its correctness and optimality. There is slow-growing community of users of ORCHIDS, mostly in France (DGA, Bertin, Thalès, EADS, ANSSI) and in Canada (UQàM). ORCHIDS is open-source. LSV serves as the maintainer, and moderator of this open-source community. We have started a program in collaboration with, and funded by the French Direction Générale de l'Armement (DGA) in 2013, to evaluate, improve and document ORCHIDS.

Objective 5 Foundations for probabilistic and non-deterministic choice

Most actual cryptographic protocols rely on coin-flipping, and the semantics of processes should in all generality include provisions for probabilistic choice. Attackers on the other hand cannot be predicted, even probabilistically, and are best modeled as some form of non-deterministic choice. We have looked at the foundational question of finding good denotational models for *mixed* choice, i.e., both probabilistic and non-deterministic choice together, on infinite domains. We looked at simulations between mixed-choice transition systems (an infinite-state generalization of Markov Decision Processes), and generalized this to *similarity measures*, which quantify how far one system is from simulating another one (CI-313). We applied a measure-theoretic variant of this theory to the static analysis of numerical programs that read imprecise data from physical sensors (CI-1, RI-40).

This research led to other advances, some theoretical: a topological duality between angelic and demonic non-determinism (RI-92), a drastically simplified proof of a vast generalization of so-called Choquet-Kendall-Matheron theorems (RI-55), a short proof of a remarkable theorem by Schröder and Simpson, the invention of QRB-domains and the result that they are stable under the probabilistic powerdomain monad (CI-185, RI-16), and a new construction of so-called continuous random variables (CI-127). All this relies on fairly deep results of topology that one could find from various, sparse sources; the book (LI-1) collects them, and then some more, and is meant to become a classical reference. Another outgrowth of the theory, based on our discovery of new results in the field of Noetherian spaces, led us to solve long open problems in the theory of well-structured transition systems (WSTS; see report on the Infini axis): adequate completions of their state spaces (CI-262), natural extensions of the Karp-Miller coverability tree procedure (CI-239, RI-29, IN-5). The invited talk (IN-13) served to explain the basic theory, and how it could be used to solve easily some decidability questions on transition systems beyond the class of WSTS.

► Scientific report of axis tempo

Objective 1 Quantitative verification

Robustness of timed systems. Standard model-checking and synthesis algorithms assume the real system behaves perfectly as specified by the (mathematical) model (e.g. the timed automaton). In particular it assumes there is no perturbations in the system. However if the system runs in a digital environment (for instance if implemented on a digital processor), or if the system controls some physical equipments, this will unlikely be the case: the analysis made on the model will hardly be transferable to the real system.

With that transfer in mind, we have developed a theory for the robustness of timed systems. The first approach consists in over-approximating the system's behaviours by enlarging the clock constraints in the automaton, and to either verify that all behaviours in the enlarged system are correct (which will then ensure that any approximated behaviour, or the implemented behaviour, will be correct), or to synthesize a controller that will guide the system and try to compensate for perturbations. The second approach consists in anticipating imprecisions in the system's behaviour (by shrinking clock constraints accordingly) to prevent for additional behaviours in the system, and to either verify that no important behaviour is lost after shrinking, or to guide the system in such a way that it never gets blocked.

These works have been published as (CI-309, CI-112, CI-99, CI-98, CI-84, IN-8, CI-50). Several journal papers are submitted. The thesis of Ocan Sankur, defended on May 24, 2013, was on that topic.

Timed automata with stochastic aspects. Many applications, *e.g.* communication protocols, require models which integrate both real-time constraints and randomized aspects. The development of such models and corresponding verification algorithms is a challenging task, since it requires combining techniques from both fields of real-time verification and probabilistic verification.

In this context our contribution is the definition of the model of stochastic timed automata and game-extensions thereof, in which both delays and discrete choices can be randomized, and the development of algorithms for their qualitative and quantitative analysis, when this is possible. We distinguish mostly two subclasses of systems for which such algorithms can be designed, the class of single-clock automata, and the class of reactive timed automata, in which no invariant can block time elapsing.

These works have been published as (CI-293, CI-271, CI-231, CI-33), and a journal paper is under submission.

Timed automata with other quantitative aspects. Time is not the only quantity of interest when modelling reactive systems: energy and other resources often have a key role when evaluating the correctness or performances of such systems. Timed automata *with observers* (a.k.a. *weighted* or *priced* timed automata) provide a way of measuring quantities during executions, and with decidable optimisation problems.

As their name indicates, observers do not play any role in the evolution of the model: they can only be used to measure quantities. We have lifted this approach to *energy constraints*, where the only valid executions are those along which the measured quantities remain within given bounds. This is one step closer to hybrid automata, but we proved that timed automata with energy constraints remain decidable when only lower-bound constraints are imposed. On the contrary, reachability becomes undecidable when both lower and upper bounds are enforced.

These results were presented as (CI-273, CI-194, CI-34), and a survey about timed automata with observers was published in Communications of the ACM (RI-49).

Parameter synthesis for hybrid automata. While traditional approaches to parameter synthesis of hybrid automata are based on the analysis of bad states or failure traces, a complementary or *inverse* method has been proposed. It uses a parameter instantiation that is known to guarantee a good behavior in order to derive a constraint on the parameters that leads to the same behavior. There are different scenarios for the application of the inverse method. If a given parameter instantiation is known to guarantee certain properties, the inverse method can be used to derive an enlarged area of the parameter space that preserves these properties, while possibly allowing for enhanced performance of the system. The inverse method can also be used to obtain a measure of coverage of the parameter space by computing the zones of equivalent behavior for each point. This approach is also known as *behavioral cartography*.

The presented algorithms have been implemented in a tool called IMITATOR (Inverse Method for Inferring Time AbstracT behaviOR). The tool has originally been developed for the analysis of timed automata. The new version HYMITATOR implements the semantics of linear hybrid automata. The manipulation of symbolic states is based on the polyhedral operations of the Parma Polyhedra Library.

Various examples, both from the literature and from the industry, have been performed.

In particular, we have performed parametric verification of abstractions of a memory circuit sold by the chipset manufacturer STMicroelectronics, as well as of the prospective flight control system of the next generation of spacecrafts designed by ASTRIUM Space Transportation.

Objective 2 Games for synthesis

Temporal logics for non-zero-sum games. Temporal logics have proven to be a convenient and powerful tool for reasoning about reactive systems, in particular in the framework of model checking. In order to take the interactions of several agents in the evolution of a complex reactive system, temporal logics have been extended with a way to specify how several agents can cooperate in order to achieve their goals. This framework is conveniently seen through an analogy with games, where the agents are players, what they can do forms the rules of the game, and what they want to achieve is their winning objective.

We defined a temporal logic for expressing rich properties of non-zero-sum games (for instance, equilibria properties, or interactions between a server and several clients), and developed algorithms for verifying such properties. These results have been published as conference papers (CI-263, CI-147, CI-37).

Distributed strategy synthesis under imperfect information. Automated synthesis of systems that are correct by construction has been a long-standing ambition of computer science. One major challenge consists in constructing complex systems out of individual components that act locally, without access to full information about the global system. In general, synthesis problems in such distributed settings are undecidable, and one needs additional assumptions about the information flow between components to obtain tractable instances.

We established generic methods for monitoring the flow of information in infinite systems, and studied conditions under which monitors can be abstracted into finite-state automata, to make them accessible to automated synthesis procedures. Another line of research is concerned with distributed strategies in systems with no centralised coordinator. Towards this, we studied coordination problems in games of infinite duration under individual rationality assumptions, such as avoidance of dominated strategies.

Results of this work have been presented in a journal article (RI-76), and as conference papers (Ch-10, CI-79)

Algorithmics for parity games. Parity games are a fundamental model for modeling and analysing discrete reactive systems. Thus, the complexity of solution procedures have a strong impact on automated verification and synthesis.

We studied the complexity of parity games from different perspectives. On the one hand, we identified graph connectivity parameters correlated with algorithmic complexity, leading to the notions of DAG width and entanglement of directed graphs. Bounding these parameters allows to solve the parity game problem efficiently. A second direction of research has been concerned with extensions to the classical model of parity games with perfect information. We developed algorithms for constructing winning strategies in games with imperfect information games, or with quantitative attributes such as counters or registers allowing affine transformations.

Results of this work have been published as conference papers (CI-260, CI-45), and as articles (RI-75, RI-32, RI-17, RI-18, RI-18, CI-273).

3 Implication de l'unité dans la formation par la recherche

- **Master Parisien de Recherche en Informatique (MPRI).** Paul Gastin (2008-2010) puis Hubert Comon (2010-2013) ont été directeurs du MPRI, qui est le principal Master d'Informatique fondamentale sur la région parisienne, co-habilité par l'ENS Cachan, l'ENS Paris, l'Ecole Polytechnique, et l'Université Paris Diderot, en convention avec les Universités Paris 6, Paris 11, Telecom Paristech et INRIA. En s'appuyant sur une équipe pédagogique regroupant environ 130 chercheurs, le MPRI offre une cinquantaine de cours couvrant les principaux domaines de l'informatique fondamentale. Les membres du LSV sont très fortement impliqués dans les enseignements du MPRI.

- **Ecoles d'été et formations à l'étranger.** Les membres du laboratoire se sont impliqués dans de nombreuses écoles internationales et formations à l'étranger dont nous citons ici les principales :
  - Dans le cadre d'une coopération Erasmus avec la Roumanie, D. Berwanger a donné un cours de 48 heures au SNS Bucuresti en mars 2010, S. Haar un cours de 6 heures au Politechnica Bucuresti en mai 2013, et D. Baelde un cours de 8 heures à l'Universitatea Iasi en juin 2013.
  - D. Berwanger, en tant que membre du comité de pilotage de GAMES, a participé à l'organisation de 3 écoles thématiques sur les Automates et les Jeux (Bertinoro, Italie en juin 2009 ; Bordeaux en mai 2011 ; Champéry, Suisse en février 2013).
  - T. Chatain, S. Haar et S. Schwoon sont intervenus dans l'Advanced Tutorial on Unfoldings, associé à la conférence Petri Nets en juin 2012 à Hambourg, et juin 2013 à Milan.
  - H. Comon-Lundh a organisé deux écoles de printemps appelées *CosyProofs* (Computational and Symbolic Proofs of Security) en avril 2009 à Tokyo et en avril 2010 à Barbizon, dans le cadre d'une collaboration franco-japonaise JST/CNRS ; il a également donné un tutorial de 3 heures (« *Logic In Computer Security* ») à la conférence LICS à New Orleans en juin 2013.
  - S. Delaune et S. Kremer ont donné des cours à une école d'été sur le vote électronique SecVote en septembre 2010 à Bertinoro (Italie).
  - S. Demri a donné un cours à l'école d'été ESSLLI (European Summer School In Logic Language and Information) à Copenhague en août 2010, ainsi que P. Schnoebelen et S. Schmitz à l'école ESSLI 2012 à Opole, Pologne.
  - P. Gastin, dans le cadre du projet franco-indien ARCUS, a co-organisé les écoles ACTS'09, ACTS'10 et ACTS'11 (Automata, Concurrency and Timed Systems), et a donné deux exposés de formation à la recherche pour WATA'10 (Weighted Automata : Theory and Applications) en mai 2010, dans le cadre du Research Training Group « *Quantitative Logics and Automata* », à Leipzig en avril 2013.

- S. Haddad a donné deux conférences à l'Advanced Course in Petri Nets (Rostock, septembre 2010), deux conférences à la PhD School du projet européen DISC (Cagliari, juin 2011) et deux conférences aux tutoriaux de la conférence Petri Nets (Hambourg, juin 2012 et Milan, juin 2013).
- L. Ségoufin, dans le cadre du projet européen FoX, a co-organisé deux écoles (5-9 oct 2009 à Dortmund, 1-3 sept 2010 à Varsovie), et a assuré un cours de 3h à l'école organisée par GAMES les 4-8 février 2013 à Champéry (Suisse).

- **Laboratoire International Associé (LIA) *INFORMEL*.** Paul Gastin est co-directeur du LIA franco-indien *INFORMEL*, avec Madhavan Mukund (CMI). Le laboratoire, fondé en 2012, fédère les activités de chercheurs du CNRS, de l'ENS Cachan de l'Université Bordeaux 1, côté français, et le Chennai Mathematical Institue (CMI), l'Institute of Mathematical Sciences Chennai (IMSc), et l'Indian Insitute od Science Bangalore (IISc), côté indien. La thématique couvre les méthodes formelles et leurs applications à la vérification des systèmes complexes. Le LIA a déjà permis de financer le stage de 3 mois de 4 étudiants indiens (CMI et IIT Bombay) en France de mai à juillet 2012, ainsi que la thèse d'un doctorant indien en co-tutelle avec Philippe Schnoebelen (LSV) et K. Narayan Kumar (CMI) depuis octobre 2012. Il a également permis d'initier des collaborations entre membres du LSV et chercheurs indiens qui ont déjà abouti aux publications communes (CI-36, CI-51).

- **Institut FARMAN.** Laurent Fribourg est directeur scientifique de l'Institut Farman qui fédère et soutient des projets inter-disciplinaires de 5 labos de l'ENS Cachan (maths appliquées, électronique, automatique, mécanique et informatique). Durant la période 2008-2013, le LSV a participé à 8 projets Farman dont 4 ont donné lieu à des publications communes avec les labos de mécanique, électronique ou automatique dans des conférences internationales (CI-68, CI-91, CO-20, RI-87). En outre, le laboratoire SATIE (électronique) en coopération avec le LSV va organiser une formation à Cachan en 2014 à destination des industriels de l'automobile et de l'électronique de puissance sur la synthèse de commande des systèmes commutés. En 2008-2013, à travers Farman, le LSV a ainsi contribué significativement à l'essor de l'inter-disciplinarité sur le campus de Cachan et à la diffusion de l'utilisation des méthodes formelles auprès de nos collègues des Sciences Pour l'Ingénieur.

4 Stratégie et perspectives scientifiques pour le futur contrat

4.1 Points forts (éléments qui soutiennent la stratégie scientifique)

- **Excellence scientifique.** L'excellence scientifique qui se traduit par des centaines de publications dans les meilleurs journaux et actes de conférences internationales, qui était déjà un de nos points forts à la dernière évaluation, s'est maintenue et même renforcée.

- **Animation scientifique.** En même temps, l'implication des membres du LSV dans l'animation et les instances d'évaluation et de pilotage de la recherche scientifique, déjà importante au dernier quadriennal, s'est considérablement accrue (dizaines d'organisation et/ou présidences d'événements internationaux, dizaines de participations à des comités AERES, deux appartenances au CoNRS, appartenances aux instances de l'INRIA). La visibilité et reconnaissance internationale se sont également spectaculairement manifestées par l'octroi de deux médailles d'argent CNRS en 2008 et 2011, un prix international EATCS Presburger 2011, un ERC starting grant 2012 et plusieurs contrats européens FP7.

- **Liens avec INRIA.** L'arrivée de Serge Abiteboul dans l'axe DAHU en 2008 a conféré, non seulement au LSV, mais également à l'ENS Cachan une visibilité mondiale, notamment lors de son cours assuré au Collège de France en 2012 (« Sciences des données : de la logique du premier ordre à la Toile »). Le partenariat avec INRIA s'est renforcé avec la création d'une 3ème équipe-projet MEXICO en 2009 sur la vérification et synthèse des architectures distribuées. De façon générale, INRIA propose des bourses de doctorants et post-doctorants qui permettent un flux des élèves de l'ENS cachan et du MPRI vers les equipes INRIA externes à Cachan, et en sens inverse, de financer des doctorats, post-docs et délégations. L'étape suivante naturelle est que INRIA devienne la 3ème co-tutelle du LSV (en sus du CNRS et de l'ENS cachan). Le processus n'a pas encore abouti pour des raisons de calendrier, mais devrait être conclu en 2014.

- **LIA INFORMEL.** En dehors du renforcement des liens avec l'INRIA, la création du LIA INFORMEL avec l'Inde et l'essor de l'Institut Farman de l'ENS cachan ont eu un grand impact sur la vie du laboratoire. Le LIA INFORMEL a été à l'origine d'un très important flux de visiteurs (professeurs, doctorants, post-doctorants) indiens au lSV et, en sens inverse, de visites longues de plusieurs mois de chercheurs du

LSV (Paul Gastin, Dietmar Berwanger,. . .) en Inde, ce qui a abouti à des coopérations très fructueuses notamment dans le domaine des jeux et systèmes distribués.

- **Institut Farman.** L'Institut Farman a permis, quant à lui, au travers d'une dizaine de projets interdisciplinaires, de faire collaborer des membres du LSV avec des membres de laboratoires d'électronique, d'automatique et de mécanique de l'ENS Cachan sur des thématiques nouvelles pour le LSV, et a permis de faire connaître l'intérêt des méthodes formelles au-delà du cercle des informaticiens.

- **Cohésion du laboratoire.** D'un point de vue organisationnel, la dispersion des membres du LSV sur quatre sites résultant de la croissance des effectifs lors de la période 2005-2008 a pris fin grâce à d'importants travaux qui ont abouti à la fusion de trois de ces sites. Notons au passage que le mode de fonctionnement et la cohésion du laboratoire se sont parfaitement maintenus durant la période 2008-2013 malgré un changement de direction en 2011. Nous en sommes redevables au type d'organisation proche et réparti mis en place dès la création, à l'esprit collectif de tous les membres, et à l'excellence du personnel ITA, en particulier de la gestionnaire du laboratoire depuis 2008.

4.2 Points à améliorer (éléments internes qui pourraient fragiliser la stratégie scientifique ou ls perspectives)

- **Encadrement.** Nous éprouvons de façon récurrente une difficulté à recruter des doctorants. Ceci est un problème général en France où les jeunes ont tendance à se détourner de la recherche scientifique. Notons que nous avons pour règle de ne pas recruter plus d'un ou deux doctorants issus de l'ENS Cachan par année.

4.3 Risques liés au contexte (éléments externes de nature à contrarier la stratégie scientifique)

- **Contacts industriels.** Après le départ de Graham Steel qui a joué un rôle moteur dans les contacts avec les industriels sur la période 2008-2012, il y a un risque certain de démobilisation du LSV vis-à-vis des contrats industriels. Ces contrats nécessitent souvent une grande énergie des chercheurs, et se heurtent à la pression exercée par les industriels sur leurs ingénieurs pour avoir des résultats en des temps trop courts de réflexion et d'échange. Nous explorons actuellement la possibilité de mutualiser ces relations industrielles au sein de l'Institut Farman en nous associant avec d'autres laboratoires de l'Institut qui semblent avoir une meilleure expérience et gestion des contrats industriels.

- **Déménagement sur le plateau de Saclay.** Le déménagement de l'ENS cachan sur le campus Paris-Saclay en 2018 est évidemment un facteur de risques. Ces risques sont multiples :
  - éloignement de Paris, carence des transports, carence des logements étudiants, difficultés conséquentes de faire venir et loger des professeurs invités ;
  - distension de nos liens avec les universités parisiennes ;
  - concurrence, partage et appauvrissement des ressources face à des disciplines mieux reconnues sur le plateau (comme les physiciens), . . .

La décision de déménagement, à laquelle le LSV n'a évidemment pris aucune part, étant actée, beaucoup d'entre nous se sont considérablement investis depuis deux ans dans les actions associées, notamment dans les multiples initiatives d'excellence (Idex, Labex, Equipex,. . .) :

- Sege Abiteboul a fait partie dès son origine du « CAC » (ancêtre du Sénat Académique), puis fait partie aujourd'hui du Sénat,

- Hubert Comon a été à l'initiative d'un premier projet de Labex, et est responsable de la commission formation de l'actuel labex Digicosme,

- Philippe Schnoebelen est responsable d'un des 3 axes scientifiques du labex Digicosme (axe SciLex : « Sûreté/Sécurité »).

En résumé, nous nous investissons, avec nos collègues du LRI, du LIX et autres laboratoires d'informatique du campus Paris-Saclay, pour faire reconnaître la discipline informatique (dénommée STIC) au travers d'un département et d'une Ecole Doctorale *unique*. Notre action se joue, non seulement au niveau institutionnel pour délimiter le périmètre de l'informatique et ses interfaces, mais au niveau scientifique pour recentrer et enrichir les champs scientifiques des laboratoires informatiques du campus. Pour prendre l'exemple de quelques pistes concrètes du LSV, l'installation sur Saclay pourrait être l'occasion de (re)collaborer avec :

- l'équipe de Catuscia Palamidessi (LIX) dans le domaine du pi-calcul probabiliste,
- l'équipe ProVal (LRI) sur la preuve de programmes, ou
- l'équipe d'Eric Goubault (CEA-LIST) sur la simulation symbolique et l'interprétation abstraite.

La prochaine relocalisation sur Saclay nous incite ainsi à monter dès aujourd'hui de nouveaux projets en commun. L'axe SciLex du labex Digicosme fournit un cadre naturel à la définition d'axes stratégiques de coopération. L'avenir des axes scientifiques du LSV est donc lié à l'élaboration des coopérations qui vont se dégager dans les 3 prochaines années.

Tout en explorant ces nouvelles opportunités associées à Saclay, le projet scientifique du LSV reste cependant fondamentalement associé aujourd'hui aux 5 axes actuels. Chaque axe a ainsi développé un projet propre qui s'inscrit dans le prolongement naturel de sa problématique et de ses travaux. Ce sont ces projets propres qui vont être maintenant exposés[5].

4.4 Projet scientifique

► Scientific project of axis dahu

For the next years we would like to distinguish three objectives.

Objective 1 Specification and verification of database driven systems

This objective aims at making systems with data safer and more reliable. This means providing suitable models together with a toolbox for helping in the design and implementation of such systems. It is a continuation of our current work and will be done in collaboration with V. Vianu (UCSD) and M. Bojańczyk (Warsaw). This objective is very broad and has many facets. During the next years we will work in particular on the following questions.

- The results we have recently obtained on the static analysis of the AXML model yields very high complexities that limit its practical impact. In the future we plan to investigate more realistic scenarios.
- We will also continue our work on automated verification of temporal properties over database driven systems. We would like to extend our previous work in order to deal with more general model of databases and include more operations on data.

Objective 2 Query processing for the Web

This objective aims at finding query languages and query processing solutions suitable for modern Web applications. This includes efficient query evaluation as well as query optimization. Besides continuing our work on the analysis of XML query languages, we will investigate two new directions, namely querying Web graph databases and enumeration techniques for query answering.

- *Query languages for graph databases.* Graph-structured data on the Web can be found in emerging applications such as *RDF* and *linked data*, or *social networks*. Classical database languages are not suitable to query such data, essentially because they do not allow to (easily) express simple connectivity queries, which are the basic building block in graph navigation. On the other hand, query languages based on reachability patterns, which have also been extensively studied, do allow graph navigation, but are too limited in the Web scenario. Extensions of these languages which support queries of interest for RDF or social network applications have been recently proposed, but they come with a high evaluation cost. Our main objective here is to study new graph query languages which guarantee efficient query evaluation and feasible optimization, still being sufficiently expressive to define typical interesting queries in the Web application context.
- *Enumeration of query answers.* We plan to continue our work on enumeration of query answers. Recall that the goal is to obtain index structures easily computable (say in linear time in the size of the database), that allow constant delay in the enumeration process. This raises many challenging fundamental questions that we would like to address. For instance we would like to understand when this enumeration process is not possible (lower bounds). We would also like to extend the cases where we already have constant delay enumeration by either considering bigger classes of structures or more powerful logics (upper bounds).

[5] en anglais, à des fins de réutilisation pour les évaluations INRIA des EPC

Objective 3 Distributed knowledge base

As a foundation for managing distribution, we are investigating the use of distributed knowledge bases to handle data and meta-data, as well as access control and localization, in a holistic integrated setting. Reasoning on a knowledge base is specified using a rule-based language supporting the exchange of rules, namely Webdamlog. This raises a number of issues such as scaling to a large number of participants, integrating with popular systems and social networks, and in general helping users with accessing data.

The approach also raises data privacy issues. Access control is well understood in a centralized setting but much less in a distributed one. We are investigating issues related to keeping some control on data access even when data circulate on a network. We also want to control the exchange of rules and the distribution of tasks.

Finally, observe that data on the Web (and in particular in a social network) are typically imprecise and uncertain. We want to investigate issues such as data integration in such a setting. This involves, for instance, understanding the alignment of entities and relations from different sources as well as that of resolving contradictions between the sources.

► Scientific project of axis infini

The main thrust for our investigations in the coming years revolves around the decidability, algorithmics and complexity of WSTS models and of the most commonly used wqos. Let us just mention three kinds of projects (involving WSTS/WQO) among all others:

Objective 1 Algorithmics of Complete WSTS/WQOs

The theory of complete wqos and complete WSTS (CI-262, CI-123, RI-29, IN-5) currently deals mostly with decidability and/or forward analysis. This field is still mostly uncovered (e.g., good data-structures for ideals have only been proposed for the two simplest wqos used in verification). We intend to pursue this topic by exploring in more depth the possibilities that have been opened: complexity of completion-based algorithms, generic data-structures for completion-based algorithms (i.e., for ideals, cones, limits), coverability trees and graphs for complete WSTS.

Objective 2 Regular Model-Checking and Complete WSTS

The completion techniques (and the new well-structured systems) open the way to regular model-checking approaches for the verification of new models. For some of them, e.g. the priority channel systems of (Ra-6), we intend to develop data-structures, acceleration techniques, and finally prototype, tools demonstrating the feasibility of automated verification.

Objective 3 Complexity Beyond Elementary

Our initial results on the complexity of problems that rely on a wqo for decidability have unearthed a surprising gap in complexity theory. When dealing with problems that are non-elementary, i.e., outside the exponential hierarchy, but still decidable, thus also outside the scope of the arithmetic and analytic hierarchies, one has no adequate framework for assessing computational complexity.[6] This is unfortunate since problems of such complexity often appear in combinatorics, logics, and verification. The consequence of this gap is that most of the work for complexity analysis has to start afresh from low-level Turing machine computations, instead of employing simpler reductions from some master problem, like SAT for NP or the Post Correspondence Problem for Σ_1. We intend to develop the adequate notions of complexity classes and reductions, and propose good master problems for such complexities. This foundational effort relates problems from different areas, in particular, problems outside verification. It will require communicating with the experts in those areas if we expect them to start using the newly-proposed complexity tools.

► Scientific project of axis mexico

The results obtained thus far point to several opportunities and leads that will govern our work over the coming years.

[6] Even Aaronson's Complexity Zoo has only Primitive-Recursive between Elementary and Recursive.

Objective 1 Models for concurrency

The study of the key models for concurrent behavior, including communicating automata, Petri nets, their variants and unfoldings, remains at the heart of MExICo's work. Moreover, the testing and diagnosis frameworks for concurrent systems will be further explored. We mention in particular recent work on active diagnosis, i.e. the synthesis of control strategies to ensure diagnosability for systems whose observability properties do not allow diagnosis without control input. For this problem, which combines challenges of diagnosis and of controller synthesis, we have recently developed a novel approach involving advanced automata theoretic constructions. Here, it will be interesting next to treat the case of several fault types, which makes the problem a multi-objective one, to compute precisely and to minimize the exact diagnosis delay; and there are many other perspectives in this direction.

Objective 2 Verification of distributed systems

In a broader view, the questions of *observability* and *opacity* of concurrent systems will be in the focus of our research, in both a logical and a probabilistic perspective. We aim at completing the formal framework for handling interaction and observation in a concurrent, partial order or compositional setting. The role of different types of *fairness* properties, witnessed already by the reveals relations researched in the MExICo team, in designing and monitoring systems, is another issue that deserves further investigation.

Specifications in partial order logics have the potential to capture subtle yet vital properties for distributed systems that involve, e.g., concurrent transactions. The MExICo team has strong expertise in these logics, and contributed to showing that for suitable restrictions of such logics, model checking and satisfiability are decidable. We are interested in pursuing research in this only partly charted territory; in particular, efficient *distributed* verification algorithms have yet to be developed.

Objective 3 Implementability

We have identified the problem of *implementation* on distributed architectures from models like Petri nets or networks of automata that describe concurrency using high-level paradigms such as multi-party rendez-vous or shared clocks. Implementing them, or simply translating them to lower-level models, requires introducing new communications e.g. to initiate a rendez-vous, or send the value of a clock. Yet the implementation should keep as much as possible of the concurrency specified in the high-level model. To tackle this problem, we first need the right tools that allow us to compare behaviours of (possibly heterogeneous) models. Classical preorders like simulation are not sufficient since they compare only sequential behaviours and do not take concurrency into account. Concurrent bisimulations exist but they are limited to fully asynchronous systems without time and without information about the decomposition in sequential components. We will have to design more powerful notions. Then we will define transformations from high-level to low-level models that show how, for each high-level communication paradigm, these can be implemented and how much communication between components they require. These transformations will then have to be validated with respect to the appropriate behavioural comparisons as above.

MExICo's work is driven by formalizable problems that are common to several application domains; we therefore continue to work on several such fields rather than a single one. Contrary to what we expected five years ago, today the field of service composition and orchestration is not fertile for industrial cooperation. However, fruitful contacts exist with telecommunications and public transport operators, in particular via the IRT SystemX in whose subproject on multi-modal transport we are involved. Over the five years to come, these fields will definitely play an important role in our work; we will seek and seize further opportunities where possible.

► Scientific project of axis secsi

Computer security is more pressing a concern as ever, and this is not going to change anytime soon. Attacks were once limited to what an isolated hacker teen did, and are now produced by gangster organizations, big firms, and government agencies alike. New threats are emerging every day, and the incredible variety of application domains of which we have already mentioned a few testifies of it.

SECSI was initially started in 2001 with the ambition of having a global view on computer security. This is no longer possible. We must therefore concentrate on a few important topics, on which we have built expertise, and on which we can hope to have an impact in the future. These topics include continuations of many questions we have addressed in the past.

Objective 1 Symbolic vs. computational models

On the *foundations of cryptographic security*, a common belief is that symbolic models are not faithful to reality, but computational models are. We have shown that there were many bridges between the two, so that symbolic models are, in fact, relatively realistic. More importantly, we have shown that even computational models have severe limitations, as the case of dishonest keys demonstrates. We strongly believe that an entirely novel approach is called for, and the symbolic model proposed in (CI-73), where what is specified is what the attacker cannot do, is certainly the right way. This has to be explored and deepened: completing a catalogue of useful impossibility assumptions, and designing efficient automated proof techniques.

Objective 2 Equivalence-based properties

A second avenue that we will pursue is on *equivalence-based properties*. As we have said already, trace-based security properties have been fairly well studied, but new issues such as *privacy* (in e-voting, the electronic passport, for example) call for entirely new models and algorithmic techniques. We have described some of the first attempts we have done in this direction. Stéphanie DELAUNE's new ANR grant VIP (`http://www.lsv.ens-cachan.fr/Projects/anr-vip/?l=en`), started January 2012, will serve as a driving force here. This covers three aspects. The first one is *models*. Already in e-voting, privacy means several different security properties, and this only gets more complicated with the consideration of other protocols with a privacy aspect: for many applications such as routing protocols or location-based services for vehicular ad hoc networks (e.g. e-toll collection, "pay-as-you-go" insurance, . . .), formal definitions of privacy are still missing. We plan to repair this. The second aspect is *algorithms* for verifying equivalence-based properties: trace versus observational equivalence, more precise approximations (than, e.g., those used in B. Blanchet's ProVerif, which are already too coarse in verifying voter anonymity in e-voting protocols), equivalence for larger classes of processes. Finally, we plan to explore *modularity*, in two directions: *combining* the decision procedures that we will obtain for various cryptographic primitives, and *composing* protocols together, even in the presence of shared secrets. We have already described some of our efforts in these directions. Applications include being able to establish privacy in the presence of two honest voters (not just one, as done now), or untraceability in presence of two different tags; in the longer term, to obtain guarantees in a setting that involves arbitrarily many voters or tags.

Objective 3 Automated proofs

Finally, we would like to explore *new proof techniques*. We have concentrated on automated security proofs, but scalability concerns will inevitably force us to design new approaches that mix automated and interactive proofs. We shall also come back to the question of certification, and the generation of formal proofs of security (in a proof assistant), which (CI-301, RI-70) pioneered in a setting restricted to secrecy, symbolic models, and completely automated formal proof generation. We plan to keep an eye on extensions to probabilistic and non-deterministic systems (on the theoretical side of which we now have considerable expertise), and on the security of implementations (both software and hardware).

► Scientific project of axis tempo

Our research project for the next five years tightly follows the research programme of two European project that the TEMPO group just got accepted: the first one is the ERC project EQualIS "Enhancing the Quality of Interacting Systems", with Patricia Bouyer as principal investigator; the second one is the FET project Cassting "Collective Adaptive System Synthesis using Non-zero-sum Games", with Nicolas Markey as the coordinator. Both projects share a common objective of developing new techniques for reasoning about and automatically synthesising complex systems, including quantitative constraints.

Objective 1 Analysis of complex interacting systems

With the development of both wired and wireless communications, an increasing number of reactive systems are now able to communicate with their surrounding systems, and to take advantage of this information in order to optimise their behaviour. These interactions make the verification process much more complex, as the objective is now to ensure correctness of the whole system for any behaviour of the surrounding systems.

Using a convenient analogy with game theory, we see the surrounding systems as an opponent player, whose role is to adapt their behaviour in order to make the system fail. Checking correctness of the system in this setting corresponds to checking that the system is always able to counteract these attacks of the environment: this precisely corresponds to checking that the system has a winning strategy in the game it plays against the neighbouring devices.

Objective 2 Automated synthesis

The verification process is mostly based on a trial-and-error approach, where a hand-crafted model of a system is checked and refined iteratively until (hopefully) a correct model is obtained. The drawback is obvious, and the automatic synthesis of a model that would be correct by construction would be an unprecedented breakthrough in model-based design.

Here again, game theory will be a convenient formalism, but we have to model each component of the system as a different player, having its own role and objective. The classical zero-sum setting, where two players have opposite objectives, is not powerful enough to model such interactions: when dealing with complex systems where many components interact, we need to move to the much richer setting of *non-zero-sum games*. This in turn requires that we move from the simple concept of winning strategies to more intricate concepts involving equilibria. Understanding what are the relevant concepts in the context of formal verification, and developing models, languages and algorithms for modelling, reasoning about and verifying such systems, are two important challenges that we will meet.

Objective 3 Measures of correctness

While most of verification techniques use boolean values, we believe that defining and evaluating *measures of correctness* of a system would be much more informative than the mere boolean value computed by the current techniques. While we think this is true of classical models (automata, ...) involving no quantitative aspects, this is even more obvious when dealing with quantitative models, such as priced and/or timed automata, and when dealing with robustness of such systems against external perturbations.

5 Bilan récapitulatif

Du 1er janvier 2008 au 30 juin 2013 :

- Les effectifs de l'unité sont passés de 21 chercheurs et enseignants-chercheurs permanents à 24 avec un flux de 7 entrants pour 4 sortants.
- Le LSV a formé 18 doctorants et 8 HDR (dont les 4 sortants).
- Le LSV a créé deux nouveaux axes correspondant à deux nouvelles équipes-projets communes (EPC) avec INRIA, passant ainsi de trois à cinq axes.
- Le LSV a été à l'initiative d'un laboratoire international associé (LIA) du CNRS avec l'Inde.
- Le LSV a contribué de façon significative au développement important de l'Institut Farman (Fédération de Recherche CNRS créée en 2007) qui coordonne les activités interdisciplinaires de cinq laboratoires sur le campus de l'ENS Cachan.
- Les membres du LSV ont écrit sur la période plusieurs centaines de publications dans les revues et actes de conférence les plus prestigieuses du domaine. Ils ont organisé ou présidé 15 conférences internationales sur la période.
- Le LSV a participé à de nombreuses instances d'évaluation et de pilotage de la Recherche (par ex., 22 participations à des comités d'évaluation AERES).
- Plusieurs membres du LSV ont reçu de prestigieuses marques de reconnaissance (par ex., deux médailles d'argent CNRS, un prix EATCS Presburger, un projet ERC Starting Grant, une chaire au Collège de France).
- Afin d'améliorer la pérennisation de ses relations industrielles, le LSV va explorer la possibilité de mutualiser ces relations avec d'autres laboratoires de l'Institut Farman.
- Le projet scientifique du LSV repose sur le socle des cinq projets propres aux axes du laboratoire, et sur l'exploration dès aujourd'hui de coopérations potentielles avec les laboratoires LIX et LRI avec qui nous participons au développement de la science informatique sur le campus de l'Université Paris-Saclay.

agence d'évaluation de la recherche et de l'enseignement supérieur

Annexe 1 :
Présentation synthétique de l'entité

Laboratoire Spécification & Vérification

Intitulé de l'unité : Laboratoire Spécification & Vérification
Nom du directeur d'unité : Laurent Fribourg

▶ Effectifs de l'entité (au début du contrat en cours)

....**8**.... enseignants-chercheurs ; ....**13**... chercheurs ; ....**4**.... techniciens, ingénieurs et autres personnels ; ...**21**... post-docs et doctorants.

▶ Personnels ayant quitté l'entité pendant le contrat en cours

....**6**.... statutaires (..**250**.. mois) ; ...**25**... doctorants (..**664**.. mois) ; ....**13**... post-docs (...**156**.. mois) ;

▶ Nombre de recrutements réalisés au cours de la période considérée et origine des personnels

....**3**.... chercheurs (2 CNRS, 1 INRIA) ; ....**4**.... enseignants-chercheurs (ENS Cachan) ; ....**4**.... ITA (3 CNRS, 1 INRIA) ; ...**23**... doctorants ; ....**13**... post-doctorants.

1 Production scientifique au cours de la période écoulée (1er janvier 2008 – 30 juin 2013)

▶ Résultats majeurs

- **Analyse d'APIs de sécurité.** Par des méthodes de reverse-engineering automatisé et de démonstration automatique, l'outil Tookan a découvert des bugs de sécurité dans des dispositifs PKCS#11 commerciaux (cartes à puce, hardware security modules, tokens de sécurité), et a ainsi mis à jour plus d'une douzaine de nouvelles attaques. Ce travail a fait l'objet d'articles dans le New York Times, le Boston Globe, le Süddeutscher Zeitung.

- **XML avec information incomplète.** Nous avons réalisé une étude systématique de l'information incomplète dans les documents XML en visant à la rendre indépendante de l'application visée. Ceci a permis d'établir des classes de description de l'information incomplète qui sont robustes et débouchent sur des solutions algorithmiques efficaces.

- **Synthèse distribuée pour systèmes à communications asynchrones.** Le problème est de dériver automatiquement un programme pour un système dont toutes les exécutions satisfont une spécification donnée et ce, quelle que soit la façon dont l'environnement se comporte. Dans le cadre des systèmes ayant un comportement asynchrone, nous avons introduit un nouveau modèle de communication par *signaux*. Nous avons montré que, dans ce cadre, le problème de synthèse est décidable pour les systèmes dont le graphe de communication est fortement connexe.

- **Robustesse des systèmes temporisés.** Nous avons proposé une méthode de synthèse des stratégies garantissant l'atteignabilité d'un état-cible pour les automates temporisés, même en présence de petites perturbations induites par l'environnement sur les valeurs nominales des délais des automates.

- **Utilisation du lemme de Dickson pour classifier la complexité des problèmes informatiques.** Nous avons montré que les quasi-ordres bien fondés peuvent être utilisés non seulement pour la preuve de terminaison d'algorithmes, mais aussi pour établir des bornes supérieures de complexité.

► Bilan quantitatif des publications de l'entité

	2008	2009	2010	2011	2012	2013 jan.-juin	Total
ouvrages, chapitres, édition d'actes	7	20	5	12	4	4	52
revues internationales	22	23	40	16	34	12	147
invitations dans des conférences internationales	4	5	5	3	5	1	23
articles dans des conférences internationales	52	61	61	65	53	24	316
thèses de doctorat ou d'habilitation	4	6	6	12	7	2	37

► Publications majeures

(CC08) H. Comon-Lundh and V. Cortier. Computational Soundness of Observational Equivalence. In CCS'08, pages 109-118. ACM Press, 2008.

(ASV09) S. Abiteboul, L. Segoufin and V. Vianu. Static Analysis of Active XML Systems. ACM Transactions on Database Systems 34(4), 2009.

(BFLM11) P. Bouyer, U. Fahrenberg, K. G. Larsen and N. Markey. Quantitative analysis of real-time systems using priced timed automata. Communications of the ACM 54(9), pages 78-87, 2011.

(BHS12) B. Bérard, S. Haddad and M. Sassolas. Interrupt Timed Automata : verification and expressiveness. Formal Methods in System Design 40(1), pages 41-87, 2012.

(CD12) K. Chatterjee and L. Doyen. Partial-Observation Stochastic Games : How to Win when Belief Fails. In LICS'12, pages 175-184. IEEE Computer Society Press, 2012.

► Documents majeurs

- **Tookan** (logiciel) : outil d'analyse automatique de dispositifs de sécurité obéissant à la norme PKCS#11. A découvert plus d'une douzaine de vulnérabilités dans des produits commerciaux. `http://secgroup.ext.dsi.unive.it/tookan/`. Licence propriétaire.

- **Orchids** (logiciel) : outil de détection et de prévention d'intrusions temps réel, efficace, multi-sources. `http://www.lsv.ens-cachan.fr/Software/orchids/v2.1/`. Licence Cecill2 (GPL).

- **Webdamlog** (logiciel) : système d'échange et de manipulation de données distribuées sur le Web, capable de gérer l'hétérogénéïté des applications et services du réseau. `http://hal.inria.fr/hal-00813300`.

- **CosyVerif** (logiciel) : plateforme fournissant l'accès à différents outils de spécification et vérification de systèmes dynamiques. `http://www.cosyverif.org/`. Licence AGPL3 and EPL1.

- **Imitator** (logiciel) : outil de synthèse de contraintes pour modèles paramétrés à base d'automates temporisés, garantissant un comportement équivalent à un comportement de référence. `http://www.lsv.ens-cachan.fr/Software/imitator/`. Licence GPL.

2 Faits illustrant le rayonnement ou l'attractivité académiques de l'entité

- **Distinctions** : chaire « *Informatique et sciences numériques* » du Collège de France attribuée à Serge Abiteboul en 2011.

- **Prix et récompenses** : médailles d'argent du CNRS décernées à Hubert Comon-Lundh (2008) et à Jean Goubault-Larrecq (2011) ; Prix Presburger décerné à Patricia Bouyer-Decitre (2011).

- **Exposés invitatés à des conférences internationales** : FSTTCS'08 (Hubert COMON-LUNDH), ICALP'10 (Jean GOUBAULT-LARRECQ), PetriNets'12 (Alain FINKEL), ICDT'13 (Luc SEGOUFIN).
- **Organisation de colloques** : Computer Security Foundation Symposium (CSF'10, CSF'11) ; Concurrency Theory (CONCUR'10) ; Temporal Representation and Reasoning (TIME'10).
- **Coordination de projets internationaux** : ERC EQualIS (« *Enhancing Quality of Interacting Systems* », Patricia BOUYER-DECITRE), ERC Webdam (« *Web Data Management* », Serge ABITEBOUL), FET FoX (« *Foundations of XML* », Luc SEGOUFIN), FET Cassting (« *Synthesis using Non-zero-sum Games* », Nicolas MARKEY), LIA INFORMEL (« *INdo-French FORmal MEthods Lab.* », Paul GASTIN).

3 Faits illustrant les interactions de l'entité avec son environnement socio-économique ou culturel

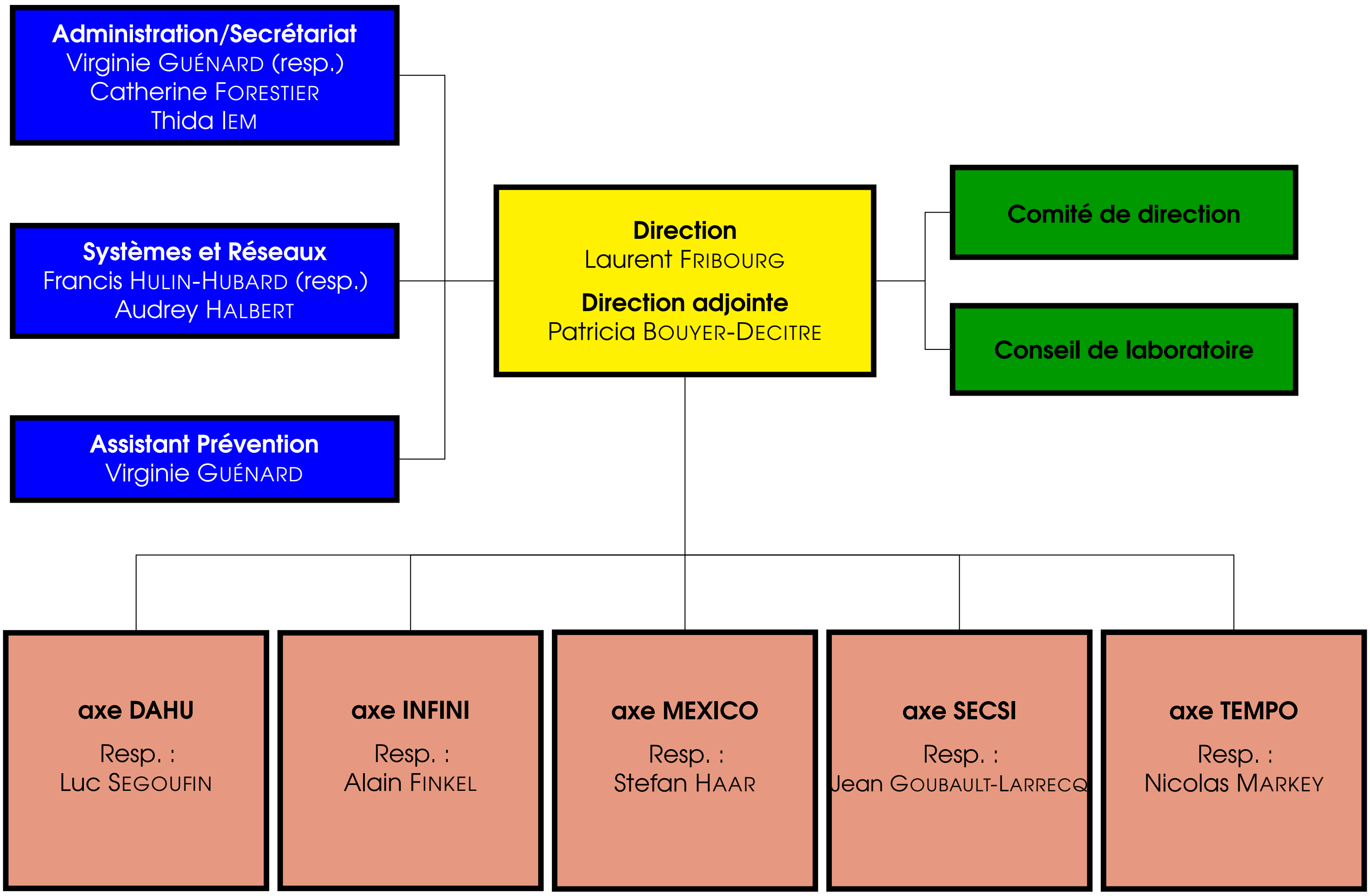
- **Nomination** : Serge ABITEBOUL a été nommé membre du Conseil National du Numérique.
- **Contrats industriels** :
  - Certificat APP Tookan en 2011, et contrats INRIA avec Boeing en 2010, Barclays en 2010, HSBC en 2011.
  - Contrat d'étude du LSV pour le cabinet AdviTech Partners en 2009 : étude de faisabilité de la startup SpidWare dans le domaine de la sécurité informatique.
  - Projet blanc CPP (confiance, preuves et probabilités) en 2009-2013 avec LSV (coordinateur), CEA Saclay, INRIA, Supélec, Dassault Systèmes, Hispano-Suiza, Safran (ex. SagemCom).
  - certificat APP Orchids délivré en 2012, suivi d'une convention INRIA-DGA sur Orchids, 2013-2016.
  - Contrat ANR VALMEM avec LSV (coordinateur), LIP6 et STMicroelectronics de 2007 à 2010 ; validation de la mémoire SPSMALL.
  - Accord CIFRE ENS Cachan-EADS : co-encadrement thèse Jean-Loup Carré (2007-2010) et participation au logiciel Penjili (propriétaire EADS) d'analyse statique de code C.
  - Contrats CIFRE avec EDF (thèse d'Arnaud Sangnier en 2008) et France Telecom/Orange (thèse de Camille Vacher en 2010).

4 Contribution à des actions de formation

- Direction du Master Parisien de Recherche en Informatique (Hubert COMON-LUNDH).
- Direction du département d'informatique de l'École Normale Supérieure de Cachan (Paul GASTIN).
- D. Berwanger a donné un cours de 48 heures au SNS Bucuresti en mars 2010 dans le cadre d'une coopération Erasmus avec la Roumanie.
- D. Berwanger a co-organisé trois écoles thématiques sur les Automates et les Jeux (Bertinoro, Italie en juin 2009 ; Bordeaux en mai 2011 ; Champéry, Suisse en février 2013).
- H. Comon-Lundh a organisé deux écoles de printemps appelées *CosyProofs* (Computational and Symbolic Proofs of Security) en avril 2009 à Tokyo et en avril 2010 à Barbizon, dans le cadre d'une collaboration franco-japonaise JST/CNRS.
- P. Gastin, dans le cadre du projet franco-indien ARCUS, a co-organisé les écoles ACTS'09, ACTS'10 et ACTS'11 (Automata, Concurrency and Timed Systems).
- L. Ségoufin, dans le cadre du projet européen FoX, a co-organisé deux écoles (5-9 oct 2009 à Dortmund, 1-3 sept 2010 à Varsovie).

agence d'évaluation de la recherche
et de l'enseignement supérieur

Annexe 4 :
Organigramme fonctionnel de l'unité



agence d'évaluation de la recherche et de l'enseignement supérieur

Annexe 6 :

Liste des publications du Laboratoire Spécification & Vérification entre le 1er janvier 2008 et le 30 juin 2013

Livres

(LI-1) Jean Goubault-Larrecq. *Non-Hausdorff Topology and Domain Theory—Selected Topics in Point-Set Topology*, volume 22 of *New Mathematical Monographs*. Cambridge University Press, March 2013.

(LI-2) Étienne André and Romain Soulat. *The Inverse Method*. Wiley-ISTE, January 2013. 176 pages.

(LI-3) Serge Abiteboul. *Sciences des données : De la logique du premier ordre à la Toile*. Leçons inaugurales du Collège de France. Fayard, 2012.

(LI-4) Serge Abiteboul, Ioana Manolescu, Philippe Rigaux, Marie-Christine Rousset, and Pierre Senellart. *Web Data Management*. Cambridge University Press, 2011.

(LI-5) Fabrizio Luccio, Linda Pagli, and Graham Steel. *Mathematical and Algorithmic Foundations of the Internet*. CRC Press, July 2011.

Chapitres de livres

(Ch-1) Marie Duflot, Marta Kwiatkowska, Gethin Norman, David Parker, Sylvain Peyronnet, Claudine Picaronny, and Jeremy Sproston. Practical applications of probabilistic model checking to communication protocols. *In* Stefania Gnesi and Tiziana Margaria, editors, *Formal Methods for Industrial Critical Systems : A Survey of Applications*, chapter 7, pages 133–150. John Wiley & Sons, Ltd. and IEEE Computer Society Press, March 2013.

(Ch-2) Jean Goubault-Larrecq and Jean-Pierre Jouannaud. The blossom of finite semantic trees. *In* Andrei Voronkov and Christoph Weidenbach, editors, *Programming Logics – Essays in Memory of Harald Ganzinger*, volume 7797 of *Lecture Notes in Computer Science*, pages 90–122. Springer, January 2013.

(Ch-3) Stéphane Demri and Paul Gastin. Specification and verification using temporal logics. *In* Deepak D'Souza and Priti Shankar, editors, *Modern applications of automata theory*, volume 2 of *IISc Research Monographs*, chapter 15, pages 457–494. World Scientific, July 2012.

(Ch-4) Hubert Comon-Lundh, Stéphanie Delaune, and Jonathan Millen. Constraint solving techniques and enriching the model with equational theories. *In* Véronique Cortier and Steve Kremer, editors, *Formal Models and Techniques for Analyzing Security Protocols*, volume 5 of *Cryptology and Information Security Series*, pages 35–61. IOS Press, 2011.

(Ch-5) Stéphane Demri and Denis Poitrenaud. Verification of infinite-state systems. *In* Serge Haddad, Fabrice Kordon, Laurent Pautet, and Laure Petrucci, editors, *Models and Analysis in Distributed Systems*, chapter 8, pages 221–269. John Wiley & Sons, Ltd., 2011.

(Ch-6) Serge Haddad. Introduction to verification. *In* Serge Haddad, Fabrice Kordon, Laurent Pautet, and Laure Petrucci, editors, *Models and Analysis in Distributed Systems*, chapter 6, pages 137–154. John Wiley & Sons, Ltd., 2011.

(Ch-7) Graham Steel. Formal analysis of security APIs. *In* Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 492–494. Springer, 2nd edition, 2011.

(Ch-8) Riccardo Focardi, Flaminia L. Luccio, and Graham Steel. An introduction to security API analysis. *In* Alessandro Aldini and Roberto Gorrieri, editors, *Foundations of Security Analysis and Design – FOSAD Tutorial Lectures (FOSAD'VI)*, volume 6858 of *Lecture Notes in Computer Science*, pages 35–65. Springer, September 2011.

(Ch-9) Laurent Doyen and Jean-François Raskin. Games with imperfect information : Theory and algorithms. *In* Krzysztof R. Apt and Erich Grädel, editors, *Lectures in Game Theory for Computer Scientists*. Cambridge University Press, January 2011.

(Ch-10) Dietmar Berwanger. Infinite coordination games. *In* Giacomo Bonnano, Benedikt Löwe, and Wiebe van der Hoek, editors, *Logic and the Foundations of Game and Decision Theory (LOFT8)*, volume 6006 of *Lecture Notes in Artificial Intelligence*, pages 1–19. Springer, 2010.

(Ch-11) Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying privacy-type properties of electronic voting protocols : A taster. *In* David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Mirosław Kutyłowski, and Ben Adida, editors, *Towards Trustworthy Elections – New Directions in Electronic Voting*, volume 6000 of *Lecture Notes in Computer Science*, pages 289–309. Springer, May 2010.

(Ch-12) Manfred Droste and Paul Gastin. Weighted automata and weighted logics. *In* Werner Kuich, Heiko Vogler, and Manfred Droste, editors, *Handbook of Weighted Automata*, EATCS Monographs in Theoretical Computer Science, chapter 5, pages 175–211. Springer, 2009.

(Ch-13) Serge Haddad. Decidability and complexity of Petri net problems. *In* Michel Diaz, editor, *Petri Nets : Fundamental Models, Verification and Applications*, pages 87–122. Wiley-ISTE, 2009.

(Ch-14) Serge Haddad and Jean-Michel Ilié. Symmetry and temporal logic. *In* Michel Diaz, editor, *Petri Nets : Fundamental Models, Verification and Applications*, pages 435–460. Wiley-ISTE, 2009.

(Ch-15) Serge Haddad and Patrice Moreaux. Stochastic Petri nets. *In* Michel Diaz, editor, *Petri Nets : Fundamental Models, Verification and Applications*, pages 269–302. Wiley-ISTE, 2009.

(Ch-16) Serge Haddad and Patrice Moreaux. Stochastic well-formed Petri nets. *In* Michel Diaz, editor, *Petri Nets : Fundamental Models, Verification and Applications*, pages 303–320. Wiley-ISTE, 2009.

(Ch-17) Serge Haddad and Patrice Moreaux. Tensor methods and stochastic Petri nets. *In* Michel Diaz, editor, *Petri Nets : Fundamental Models, Verification and Applications*, pages 321–346. Wiley-ISTE, 2009.

(Ch-18) Serge Haddad and François Vernadat. Analysis methods for Petri nets. *In* Michel Diaz, editor, *Petri Nets : Fundamental Models, Verification and Applications*, pages 41–86. Wiley-ISTE, 2009.

(Ch-19) Serge Haddad and François Vernadat. Verification of specific properties. *In* Michel Diaz, editor, *Petri Nets : Fundamental Models, Verification and Applications*, pages 349–414. Wiley-ISTE, 2009.

(Ch-20) Franck Cassez and Nicolas Markey. Control of timed systems. *In* Claude Jard and Olivier H. Roux, editors, *Communicating Embedded Systems – Software and Design*, chapter 3, pages 83–120. Wiley-ISTE, October 2009.

(Ch-21) Alexandre David, Gerd Behrmann, Peter Bulychev, Joakin Byg, Thomas Chatain, Kim G. Larsen, Paul Pettersson, Jacob Illum Rasmussen, Jiří Srba, Wang Yi, Kenneth Y. Joergensen, Didier Lime, Morgan Magnin, Olivier H. Roux, and Louis-Marie Traonouez. Tools for model-checking timed systems. *In* Claude Jard and Olivier H. Roux, editors, *Communicating Embedded Systems – Software and Design*, chapter 6, pages 165–225. Wiley-ISTE, October 2009.

(Ch-22) Susanna Donatelli and Serge Haddad. Quantitative verification of Markov chains. *In* Claude Jard and Olivier H. Roux, editors, *Communicating Embedded Systems – Software and Design*, chapter 5, pages 139–163. Wiley-ISTE, October 2009.

(Ch-23) Reynald Affeldt and Hubert Comon-Lundh. Verification of security protocols with a bounded number of sessions based on resolution for rigid variables. *In* Véronique Cortier, Claude Kirchner, Mitsuhiro Okada, and Hideki Sakurada, editors, *Formal to Practical Security*, volume 5458 of *Lecture Notes in Computer Science*, pages 1–20. Springer, May 2009.

(Ch-24) Amal El Fallah Seghrouchni and Serge Haddad. Interopérabilité des systèmes multi-agents à l'aide des services web. *In* Amal El Fallah Seghrouchni and Jean-Pierre Briot, editors, *Technologies des systèmes multi-agents et applications industrielles*, chapter 3, pages 77–99. Hermès, April 2009.

(Ch-25) Patricia Bouyer and Antoine Petit. On extensions of timed automata. *In* Kamal Lodaya, Madhavan Mukund, and R. Ramanujam, editors, *Perspectives in Concurrency Theory*, IARCS-Universities, pages 35–63. Universities Press, January 2009.

(Ch-26) Volker Diekert and Paul Gastin. Local safety and local liveness for distributed systems. *In* Kamal Lodaya, Madhavan Mukund, and R. Ramanujam, editors, *Perspectives in Concurrency Theory*, IARCS-Universities, pages 86–106. Universities Press, January 2009.

(Ch-27) Paul Gastin, Madhavan Mukund, and K. Narayan Kumar. Reachability and boundedness in time-constrained MSC graphs. *In* Kamal Lodaya, Madhavan Mukund, and R. Ramanujam, editors, *Perspectives in Concurrency Theory*, IARCS-Universities, pages 157–183. Universities Press, January 2009.

(Ch-28) Volker Diekert and Paul Gastin. First-order definable languages. *In* Jörg Flum, Erich Grädel, and Thomas Wilke, editors, *Logic and Automata : History and Perspectives*, volume 2 of *Texts in Logic and Games*, pages 261–306. Amsterdam University Press, 2008.

(Ch-29) Franck Cassez and Nicolas Markey. Contrôle des systèmes temporisés. *In* Olivier H. Roux and Claude Jard, editors, *Approches formelles des systèmes embarqués communicants*, chapter 4, pages 105–144. Hermès, October 2008.

(Ch-30) Susanna Donatelli and Serge Haddad. Vérification quantitative de chaînes de Markov. *In* Olivier H. Roux and Claude Jard, editors, *Approches formelles des systèmes embarqués communicants*, chapter 6, pages 177–198. Hermès, October 2008.

(Ch-31) Patricia Bouyer and François Laroussinie. Model checking timed automata. *In* Stephan Merz and Nicolas Navet, editors, *Modeling and Verification of Real-Time Systems*, pages 111–140. ISTE Ltd. – John Wiley & Sons, Ltd., January 2008.

(Ch-32) Serge Haddad and Patrice Moreaux. Verification of probabilistic systems methods and tools. *In* Stephan Merz and Nicolas Navet, editors, *Modeling and Verification of Real-Time Systems*, pages 289–318. ISTE Ltd. – John Wiley & Sons, Ltd., January 2008.

Édition d'ouvrages collectifs

(Ed-1) Alain Finkel, Jérôme Leroux, and Igor Potapov, editors. *Proceedings of the 6th International Wokshop on Reachability Problems (RP'12)*, volume 7550 of *Lecture Notes in Computer Science*. Springer.

(Ed-2) Serge Haddad and Lucia Pomello, editors. *Proceedings of the 33rd International Conference on Applications and Theory of Petri Nets (ICATPN'12)*, volume 7347 of *Lecture Notes in Computer Science*. Springer.

(Ed-3) Véronique Cortier and Steve Kremer, editors. *Formal Models and Techniques for Analyzing Security Protocols*, volume 5 of *Cryptology and Information Security Series*. IOS Press, 2011.

(Ed-4) Serge Haddad, Fabrice Kordon, Laurent Pautet, and Laure Petrucci, editors. *Distributed Systems Design and Algorithms*. John Wiley & Sons, Ltd., 2011.

(Ed-5) Serge Haddad, Fabrice Kordon, Laurent Pautet, and Laure Petrucci, editors. *Models and Analysis in Distributed Systems*. John Wiley & Sons, Ltd., 2011.

(Ed-6) Serge Abiteboul, Klemens Böhm, Christoph Koch, and Kian-Lee Tan. Proceedings of the 27th International Conference on Data Engineering (ICDE'11). *In* Serge Abiteboul, Klemens Böhm, Christoph Koch, and Kian-Lee Tan, editors, *Proceedings of the 27th International Conference on Data Engineering (ICDE'11), Hannover, Germany, April 2011*. IEEE Computer Society Press.

(Ed-7) Nicolas Markey and Jef Wijsen, editors. *Proceedings of the 17th International Symposium on Temporal Representation and Reasoning (TIME'10)*. IEEE Computer Society Press.

(Ed-8) Paul Gastin and François Laroussinie, editors. *Proceedings of the 21st International Conference on Concurrency Theory (CONCUR'10)*, volume 6269 of *Lecture Notes in Computer Science*. Springer.

(Ed-9) Luc Segoufin, editor. *Proceedings of the 13th International Conference on Database Theory (ICDT'10)*.

(Ed-10) Michele Boreale and Steve Kremer, editors. *Proceedings of the 7th International Workshop on Security Issues in Concurrency (SecCo'09)*, volume 7 of *Electronic Proceedings in Theoretical Computer Science*.

(Ed-11) Steve Kremer and Prakash Panangaden, editors. *Proceedings of the 6th International Workshop on Security Issues in Concurrency (SecCo'08)*, volume 242(3) of *Electronic Notes in Theoretical Computer Science*. Elsevier Science Publishers, August 2009.

(Ed-12) Peter Habermehl and Tomáš Vojnar, editors. *Joint Proceedings of the 8th, 9th and 10th International Workshops on Verification of Infinite State Systems (INFINITY'06,'07,'08)*, volume 239 of *Electronic Notes in Theoretical Computer Science*. Elsevier Science Publishers, July 2009.

(Ed-13) Carlos Areces and Stéphane Demri, editors. *Proceedings of the 5th International Workshop on Methods for Modalities (M4M-5)*, volume 231 of *Electronic Notes in Theoretical Computer Science*. Elsevier Science Publishers, March 2009.

(Ed-14) Liqun Chen, Steve Kremer, and Mark D. Ryan, editors. *Formal Protocol Verification Applied*, volume 07421 of *Dagstuhl Seminar Proceedings*.

(Ed-15) Stéphane Demri and Christian S. Jensen, editors. *Proceedings of the 15th International Symposium on Temporal Representation and Reasoning (TIME'08)*. IEEE Computer Society Press.

Articles dans des revues internationales avec comité de lecture

(RI-1) Sandie Balaguer, Thomas Chatain, and Stefan Haar. Building occurrence nets from reveals relations. *Fundamenta Informaticae*, 123(3):245–272, 2013.

(RI-2) Stéphane Demri. On selective unboundedness of VASS. *Journal of Computer and System Sciences*, 79(5):689–713, 2013.

(RI-3) Serge Haddad, Jean Mairesse, and Hoang-Thach Nguyen. Synthesis and analysis of product-form Petri nets. *Fundamenta Informaticae*, 122(1-2):147–172, 2013.

(RI-4) S. Akshay, Benedikt Bollig, and Paul Gastin. Event-clock message passing automata : A logical characterization and an emptiness checking algorithm. *Formal Methods in System Design*, 42(3):262–300, June 2013.

(RI-5) Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. Deciding equivalence-based properties using constraint solving. *Theoretical Computer Science*, 492:1–39, June 2013.

(RI-6) Paul Gastin and Nathalie Sznajder. Fair synthesis for asynchronous distributed systems. *ACM Transactions on Computational Logic*, 14(2 :9), June 2013.

(RI-7) Étienne André, Laurent Fribourg, and Jeremy Sproston. An extension of the inverse method to probabilistic timed automata. *Formal Methods in System Design*, 42(2):119–145, April 2013.

(RI-8) Luis Barguñó, Carles Creus, Guillem Godoy, Florent Jacquemard, and Camille Vacher. Decidable classes of tree automata mixing local and global constraints modulo flat theories. *Logical Methods in Computer Science*, 9(2), April 2013.

(RI-9) Rémi Bonnet, Alain Finkel, Serge Haddad, and Fernando Rosa-Velardo. Ordinal theory for expressiveness of well-structured transition systems. *Information and Computation*, 224:1–22, March 2013.

(RI-10) Mathieu Baudet, Véronique Cortier, and Stéphanie Delaune. YAPA : A generic tool for computing intruder knowledge. *ACM Transactions on Computational Logic*, 14(1 :4), February 2013.

(RI-11) Béatrice Bérard, Franck Cassez, Serge Haddad, Didier Lime, and Olivier H. Roux. The expressive power of time Petri nets. *Theoretical Computer Science*, 474:1–20, February 2013.

(RI-12) Laurent Fribourg and Ulrich Kühne. Parametric verification and test coverage for hybrid automata using the inverse method. *International Journal of Foundations of Computer Science*, 24(2):233–249, February 2013.

(RI-13) Rémi Bonnet, Alain Finkel, Jérôme Leroux, and Marc Zeitoun. Model checking vector addition systems with one zero-test. *Logical Methods in Computer Science*, 8(2 :11), 2012.

(RI-14) Dorsaf Elhog-Benzina, Serge Haddad, and Rolf Hennicker. Refinement and asynchronous composition of modal Petri nets. *In Transactions on Petri Nets and Other Models of Concurrency V*, volume 6900 of *Lecture Notes in Computer Science*, pages 96–120. Springer, 2012.

(RI-15) Diego Figueira. Alternating register automata on finite words and trees. *Logical Methods in Computer Science*, 8(1 :22), 2012.

(RI-16) Jean Goubault-Larrecq. QRB-domains and the probabilistic powerdomain. *Logical Methods in Computer Science*, 8(1 :14), 2012.

(RI-17) Dietmar Berwanger, Erich Grädel, Łukasz Kaiser, and Roman Rabinovich. Entanglement and the complexity of directed graphs. *Theoretical Computer Science*, 463:2–25, December 2012.

(RI-18) Dietmar Berwanger and Olivier Serre. Parity games on undirected graphs. *Information Processing Letters*, 112(23):928–932, December 2012.

(RI-19) Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. Bounded Parikh automata. *International Journal of Foundations of Computer Science*, 23(8):1691–1710, December 2012.

(RI-20) Paul Gastin and Nathalie Sznajder. Decidability of well-connectedness for distributed synthesis. *Information Processing Letters*, 112(24):963–968, December 2012.

(RI-21) Stefan Haar. What topology tells us about diagnosability in partial order semantics. *Discrete Event Dynamic Systems : Theory and Applications*, 22(4):383–402, December 2012.

(RI-22) Matthew Anderson, Dieter van Melkebeek, Nicole Schweikardt, and Luc Segoufin. Locality from circuit lower bounds. *SIAM Journal on Computing*, 41(6):1481–1523, November 2012.

(RI-23) Krishnendu Chatterjee and Laurent Doyen. Energy parity games. *Theoretical Computer Science*, 458:49–60, November 2012.

(RI-24) Dario Faggioli, Giuseppe Lipari, and Tommaso Cucinotta. Analysis and implementation of the multiprocessor bandwidth inheritance protocol. *Real-Time Systems*, 48(6):789–825, November 2012.

(RI-25) Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. Affine parikh automata. *RAIRO Informatique Théorique et Applications*, 46(4):511–545, October 2012.

(RI-26) Philippe Darondeau, Stéphane Demri, Roland Meyer, and Christophe Morvan. Petri net reachability graphs : Decidability status of FO properties. *Logical Methods in Computer Science*, 8(4 :9), October 2012.

(RI-27) Stéphane Demri, Deepak D'Souza, and Régis Gascon. Temporal logics of repeating values. *Journal of Logic and Computation*, 22(5):1059–1096, October 2012.

(RI-28) Mikołaj Bojańczyk, Luc Segoufin, and Howard Straubing. Piecewise testable tree languages. *Logical Methods in Computer Science*, 8(3 :26), September 2012.

(RI-29) Alain Finkel and Jean Goubault-Larrecq. Forward analysis for WSTS, part II : Complete WSTS. *Logical Methods in Computer Science*, 8(3 :28), September 2012.

(RI-30) Rodrigo M. Santos, Giuseppe Lipari, Enrico Bini, and Tommaso Cucinotta. On-line schedulability tests for adaptive reservations in fixed priority scheduling. *Real-Time Systems*, 48(5):601–634, September 2012.

(RI-31) Paolo Baldan, Alessandro Bruni, Andrea Corradini, Barbara König, César Rodríguez, and Stefan Schwoon. Efficient unfolding of contextual Petri nets. *Theoretical Computer Science*, 449(1):2–22, August 2012.

(RI-32) Dietmar Berwanger, Anuj Dawar, Paul Hunter, Staphan Kreutzer, and Jan Obdrzálek. The DAG-width of directed graphs. *Journal of Combinatorial Theory, Series B*, 102(4):900–923, July 2012.

(RI-33) Patricia Bouyer, Nicolas Markey, Joël Ouaknine, Philippe Schnoebelen, and James Worrell. On termination and invariance for faulty channel systems. *Formal Aspects of Computing*, 24(4-6):595–607, July 2012.

(RI-34) Sandie Balaguer, Thomas Chatain, and Stefan Haar. A concurrency-preserving translation from time Petri nets to networks of timed automata. *Formal Methods in System Design*, 40(3):330–355, June 2012.

(RI-35) Benedikt Bollig and Dietrich Kuske. An optimal construction of Hanf sentences. *Journal of Applied Logic*, 10(2):179–186, June 2012.

(RI-36) Serge Abiteboul, Pierre Bourhis, and Victor Vianu. Comparing workflow specification languages : A matter of views. *ACM Transactions on Database Systems*, 37(2 :10), May 2012.

(RI-37) Véronique Cortier and Stéphanie Delaune. Decidability and combination results for two notions of knowledge in security protocols. *Journal of Automated Reasoning*, 48(4):441–487, April 2012.

(RI-38) Pierre Ganty, Rupak Majumdar, and Benjamin Monmege. Bounded underapproximations. *Formal Methods in System Design*, 40(2):206–231, April 2012.

(RI-39) Adel Bouhoula and Florent Jacquemard. Sufficient completeness verification for conditional and constrained TRS. *Journal of Applied Logic*, 10(1):127–143, March 2012.

(RI-40) Olivier Bouissou, Éric Goubault, Jean Goubault-Larrecq, and Sylvie Putot. A generalization of P-boxes to affine arithmetic, and applications to static analysis of programs. *Computing*, 94(2-4):189–201, March 2012.

(RI-41) Béatrice Bérard, Serge Haddad, and Mathieu Sassolas. Interrupt timed automata : verification and expressiveness. *Formal Methods in System Design*, 40(1):41–87, February 2012.

(RI-42) Rémi Brochenin, Stéphane Demri, and Étienne Lozes. On the almighty wand. *Information and Computation*, 211:106–137, February 2012.

(RI-43) Ştefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. Computing knowledge in security protocols under convergent equational theories. *Journal of Automated Reasoning*, 48(2):219–262, February 2012.

(RI-44) Stéphane Demri, Marcin Jurdziński, Oded Lachish, and Ranko Lazić. The covering and boundedness problems for branching vector addition systems. *Journal of Computer and System Sciences*, 79(1):23–38, February 2012.

(RI-45) Steve Kremer, Antoine Mercier, and Ralf Treinen. Reducing equational theories for the decision of static equivalence. *Journal of Automated Reasoning*, 2(48):197–217, February 2012.

(RI-46) Assalé Adjé, Stéphane Gaubert, and Éric Goubault. Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. *Logical Methods in Computer Science*, 8(1 :1), January 2012.

(RI-47) Thomas Place and Luc Segoufin. A decidable characterization of locally testable tree languages. *Logical Methods in Computer Science*, 7(4 :03), November 2011.

(RI-48) Marco Beccuti, Giuliana Franceschinis, and Serge Haddad. MDWNsolver : A framework to design and solve Markov decision Petri nets. *International Journal of Performability Engineering*, 7(5):417–428, September 2011.

(RI-49) Patricia Bouyer, Uli Fahrenberg, Kim G. Larsen, and Nicolas Markey. Quantitative analysis of real-time systems using priced timed automata. *Communications of the ACM*, 54(9):78–87, September 2011.

(RI-50) Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. Power of randomization in automata on infinite strings. *Logical Methods in Computer Science*, 7(3 :22), September 2011.

(RI-51) Michael Ummels and Dominik Wojtczak. The complexity of Nash equilibria in stochastic multiplayer games. *Logical Methods in Computer Science*, 7(3 :20), September 2011.

(RI-52) Mikołaj Bojańczyk, Claire David, Anca Muscholl, Thomas Schwentick, and Luc Segoufin. Two-variable logic on data words. *ACM Transactions on Computational Logic*, 12(4 :27), July 2011.

(RI-53) Carlos Areces, Diego Figueira, Santiago Figueira, and Sergio Mera. The expressive power of memory logics. *Review of Symbolic Logic*, 4(2):290 – 318, June 2011.

(RI-54) Michael Backes, Iliano Cervesato, Aaron Jaggard, Andre Scedrov, and Joe-Kai Tsay. Cryptographically sound security proofs for basic and public-key Kerberos. *International Journal on Information Security*, 10(2):107–134, June 2011.

(RI-55) Jean Goubault-Larrecq and Klaus Keimel. Choquet-Kendall-Matheron theorems for non-Hausdorff spaces. *Mathematical Structures in Computer Science*, 21(3):511–561, June 2011.

(RI-56) Wojciech Kazana and Luc Segoufin. First-order query evaluation on structures of bounded degree. *Logical Methods in Computer Science*, 7(2 :20), June 2011.

(RI-57) Leonid Libkin and Cristina Sirangelo. Data exchange and schema mappings in open and closed worlds. *Journal of Computer and System Sciences*, 77(3):542–571, May 2011.

(RI-58) Patricia Bouyer, Franck Cassez, and François Laroussinie. Timed modal logics for real-time systems : Specification, verification and control. *Journal of Logic, Language and Information*, 20(2):169–203, April 2011.

(RI-59) Lubos Brim, Jakub Chaloupka, Laurent Doyen, Raffaella Gentilini, and Jean-François Raskin. Faster algorithms for mean-payoff games. *Formal Methods in System Design*, 38(2):97–118, April 2011.

(RI-60) Jean Goubault-Larrecq. Musings around the geometry of interaction, and coherence. *Theoretical Computer Science*, 412(20):1998–2014, April 2011.

(RI-61) Florent Jacquemard, Francis Klay, and Camille Vacher. Rigid tree automata. *Information and Computation*, 209(3):486–512, March 2011.

(RI-62) Souheib Baarir, Marco Beccuti, Claude Dutheillet, Giuliana Franceschinis, and Serge Haddad. Lumping partially symmetrical stochastic models. *Performance Evaluation*, 76:21–44, January 2011.

(RI-63) Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, and Martin Leucker. SMA—the smyle modeling approach. *Computing and Informatics*, 29(1):45–72, 2010.

(RI-64) Krishnendu Chatterjee, Laurent Doyen, and Thomas A. Henzinger. Quantitative languages. *ACM Transactions on Computational Logic*, 11(4), 2010.

(RI-65) Stéphane Demri, Alain Finkel, Valentin Goranko, and Govert van Drimmelen. Model-checking CTL* over flat Presburger counter systems. *Journal of Applied Non-Classical Logics*, 20(4):313–344, 2010.

(RI-66) Pablo Barceló, Leonid Libkin, Antonella Poggi, and Cristina Sirangelo. XML with incomplete information. *Journal of the ACM*, 58(1), December 2010.

(RI-67) Stéphane Demri and Alexander Rabinovich. The complexity of linear-time temporal logic over the class of ordinals. *Logical Methods in Computer Science*, 6(4), December 2010.

(RI-68) Delphine Longuet, Marc Aiguier, and Pascale Le Gall. Proof-guided test selection from first-order specifications with equality. *Journal of Automated Reasoning*, 45(4):437–473, December 2010.

(RI-69) Stéphanie Delaune, Steve Kremer, and Graham Steel. Formal analysis of PKCS#11 and proprietary extensions. *Journal of Computer Security*, 18(6):1211–1245, November 2010.

(RI-70) Jean Goubault-Larrecq. Finite models for formal security proofs. *Journal of Computer Security*, 18(6):1247–1299, November 2010.

(RI-71) Steve Kremer and Laurent Mazaré. Computationally sound analysis of protocols using bilinear pairings. *Journal of Computer Security*, 18(6):999–1033, November 2010.

(RI-72) Ruggero Lanotte, Andrea Maggiolo-Schettini, and Angelo Troina. Weak bisimulation for probabilistic timed automata ? *Theoretical Computer Science*, 411(50):4291–4322, November 2010.

(RI-73) Shuhao Li, Sandie Balaguer, Alexandre David, Kim G. Larsen, Brian Nielsen, and Saulius Pusinskas. Scenario-based verification of real-time systems using UPPAAL. *Formal Methods in System Design*, 37(2-3):200–264, November 2010.

(RI-74) Paolo Baldan, Thomas Chatain, Stefan Haar, and Barbara König. Unfolding-based diagnosis of systems with an evolving topology. *Information and Computation*, 208(10):1169–1192, October 2010.

(RI-75) Dietmar Berwanger, Krishnendu Chatterjee, Laurent Doyen, Martin De Wulf, and Thomas A. Henzinger. Strategy construction for parity games with imperfect information. *Information and Computation*, 208(10):1206–1220, October 2010.

(RI-76) Dietmar Berwanger and Łukasz Kaiser. Information tracking in games on graphs. *Journal of Logic, Language and Information*, 19(4):395–412, October 2010.

(RI-77) Mikołaj Bojańczyk and Luc Segoufin. Tree languages defined in first-order logic with one quantifier alternation. *Logical Methods in Computer Science*, 6(4 :1), October 2010.

(RI-78) Stefan Haar. Types of asynchronous diagnosability and the *reveals*-relation in occurrence nets. *IEEE Transactions on Automatic Control*, 55(10):2310–2320, October 2010.

(RI-79) Mathieu Baudet, Bogdan Warinschi, and Martín Abadi. Guessing attacks and the computational soundness of static equivalence. *Journal of Computer Security*, 18(5):909–968, September 2010.

(RI-80) Benedikt Bollig, Dietrich Kuske, and Ingmar Meinecke. Propositional dynamic logic for message-passing systems. *Logical Methods in Computer Science*, 6(3 :16), September 2010.

(RI-81) Krishnendu Chatterjee, Laurent Doyen, and Thomas A. Henzinger. Expressiveness and closure properties for quantitative languages. *Logical Methods in Computer Science*, 6(3 :10), September 2010.

(RI-82) Stéphane Demri and Denis Lugiez. Complexity of modal logics with Presburger constraints. *Journal of Applied Logic*, 8(3):233–252, September 2010.

(RI-83) Étienne Lozes and Jules Villard. A spatial equational logic for the applied π-calculus. *Distributed Computing*, 23(1):61–83, September 2010.

(RI-84) Pierre-Cyrille Héam, Cyril Nicaud, and Sylvain Schmitz. Parametric random generation of deterministic tree automata. *Theoretical Computer Science*, 411(38-39):3469–3480, August 2010.

(RI-85) Paul Gastin and Dietrich Kuske. Uniform satisfiability problem for local temporal logics over Mazurkiewicz traces. *Information and Computation*, 208(7):797–816, July 2010.

(RI-86) Alan Nash, Luc Segoufin, and Victor Vianu. Views and queries : Determinacy and rewriting. *ACM Transactions on Database Systems*, 35(3), July 2010.

(RI-87) Thomas Brihaye, Marc Jungers, Samson Lasaulce, Nicolas Markey, and Ghassan Oreiby. Using model checking for analyzing distributed power control problems. *EURASIP Journal on Wireless Communications and Networking*, 2010(861472), June 2010.

(RI-88) Leonid Libkin and Cristina Sirangelo. Reasoning about XML with temporal logics and automata. *Journal of Applied Logic*, 8(2):210–232, June 2010.

(RI-89) Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, and Martin Leucker. Learning communicating automata from MSCs. *IEEE Transactions on Software Engineering*, 36(3):390–408, May-June 2010.

(RI-90) Stéphane Demri, Ranko Lazić, and Arnaud Sangnier. Model checking memoryful linear-time logics over one-counter automata. *Theoretical Computer Science*, 411(22-24):2298–2316, May 2010.

(RI-91) Véronique Cortier, Steve Kremer, and Bogdan Warinschi. A survey of symbolic methods in computational analysis of cryptographic systems. *Journal of Automated Reasoning*, 46(3-4):225–259, April 2010.

(RI-92) Jean Goubault-Larrecq. De Groot duality and models of choice : Angels, demons, and nature. *Mathematical Structures in Computer Science*, 20(2):169–237, April 2010.

(RI-93) Laura Recalde, Serge Haddad, and Manuel Silva. Continuous Petri nets : Expressive power and decidability issues. *International Journal of Foundations of Computer Science*, 21(2):235–256, April 2010.

(RI-94) Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Symbolic bisimulation for the applied pi calculus. *Journal of Computer Security*, 18(2):317–377, March 2010.

(RI-95) Balder ten Cate and Luc Segoufin. Transitive closure logic, nested tree walking automata, and XPath. *Journal of the ACM*, 57(3), March 2010.

(RI-96) Adam Antonik, Michael Huth, Kim G. Larsen, Ulrik Nyman, and Andrzej Wąsowski. Modal and mixed specifications : key decision problems and their complexities. *Mathematical Structures in Computer Science*, 10(1):75–103, February 2010.

(RI-97) Patricia Bouyer, Fabrice Chevalier, and Nicolas Markey. On the expressiveness of TPTL and MTL. *Information and Computation*, 208(2):97–116, February 2010.

(RI-98) Pierre Arnoux and Alain Finkel. Using mental imagery processes for teaching and research in mathematics and computer science. *International Journal of Mathematical Education in Science and Technology*, 41(2):229–242, January 2010.

(RI-99) Patricia Bouyer, Thomas Brihaye, and Fabrice Chevalier. O-minimal hybrid reachability games. *Logical Methods in Computer Science*, 6(1 :1), January 2010.

(RI-100) Hubert Comon-Lundh, Véronique Cortier, and Eugen Zălinescu. Deciding security properties for cryptographic protocols. application to key cycles. *ACM Transactions on Computational Logic*, 11(2), January 2010.

(RI-101) Leonid Libkin and Cristina Sirangelo. Disjoint pattern matching and implication in strings. *Information Processing Letters*, 110(4):143–147, January 2010.

(RI-102) Sylvain Schmitz. An experimental ambiguity detection tool. *Science of Computer Programming*, 75(1-2):71–84, January 2010.

(RI-103) Patricia Bouyer, Serge Haddad, and Pierre-Alain Reynier. Undecidability results for timed automata with silent transitions. *Fundamenta Informaticae*, 92(1-2):1–25, 2009.

(RI-104) Serge Abiteboul, Luc Segoufin, and Victor Vianu. Static analysis of Active XML systems. *ACM Transactions on Database Systems*, 34(4), December 2009.

(RI-105) Patricia Bouyer, Thomas Brihaye, and Fabrice Chevalier. Weighted o-minimal hybrid systems. *Annals of Pure and Applied Logics*, 161(3):268–288, December 2009.

(RI-106) Rémi Brochenin, Stéphane Demri, and Étienne Lozes. Reasoning about sequences of memory states. *Annals of Pure and Applied Logics*, 161(3):305–323, December 2009.

(RI-107) Fabrice Chevalier, Deepak D'Souza, M. Raj Mohan, and Pavithra Prabhakar. Automata and logics over finitely varying functions. *Annals of Pure and Applied Logics*, 161(3):324–336, December 2009.

(RI-108) Stéphane Demri and Régis Gascon. The effects of bounding syntactic resources on Presburger LTL. *Journal of Logic and Computation*, 19(6):1541–1575, December 2009.

(RI-109) Serge Abiteboul, Benny Kimelfeld, Yehoshua Sagiv, and Pierre Senellaert. On the expressiveness of probabilistic XML models. *The VLDB Journal*, 18(5):1041–1064, October 2009.

(RI-110) Étienne André, Thomas Chatain, Emmanuelle Encrenaz, and Laurent Fribourg. An inverse method for parametric timed automata. *International Journal of Foundations of Computer Science*, 20(5):819–836, October 2009.

(RI-111) Michael Benedikt and Luc Segoufin. Regular tree languages definable in FO and in FO_{mod}. *ACM Transactions on Computational Logic*, 11(1), October 2009.

(RI-112) Yohan Boichut, Roméo Courbis, Pierre-Cyrille Héam, and Olga Kouchnarenko. Handling non-left linear rules when completing tree automata. *International Journal of Foundations of Computer Science*, 20(5):837–849, October 2009.

(RI-113) Serge Abiteboul, Luc Segoufin, and Victor Vianu. Modeling and verifying active XML artifacts. *IEEE Data Engineering Bulletin*, 32(3):10–15, September 2009.

(RI-114) Céline Boutrous-Saab, Demba Coulibaly, Serge Haddad, Tarek Melliti, Patrice Moreaux, and Sylvain Rampacek. An integrated framework for web services orchestration. *International Journal of Web Services Research*, 6(4):1–29, September 2009.

(RI-115) Bogdan Cautis, Serge Abiteboul, and Tova Milo. Reasoning about XML update constraints. *Journal of Computer and System Sciences*, 75(6):336–358, September 2009.

(RI-116) Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, July 2009.

(RI-117) Serge Abiteboul and Neoklis Polyzotis. Searching shared content in communities with the data ring. *IEEE Data Engineering Bulletin*, 32(2):44–51, June 2009.

(RI-118) Paul Gastin, Nathalie Sznajder, and Marc Zeitoun. Distributed synthesis for well-connected architectures. *Formal Methods in System Design*, 34(3):215–237, June 2009.

(RI-119) Mikołaj Bojańczyk, Anca Muscholl, Thomas Schwentick, and Luc Segoufin. Two-variable logic on data trees and applications to XML reasoning. *Journal of the ACM*, 56(3), May 2009.

(RI-120) Mathieu Baudet, Véronique Cortier, and Steve Kremer. Computationally sound implementations of equational theories against passive adversaries. *Information and Computation*, 207(4):496–520, April 2009.

(RI-121) Stéphane Demri and Ranko Lazić. LTL with the freeze quantifier and register automata. *ACM Transactions on Computational Logic*, 10(3), April 2009.

(RI-122) Michael Benedikt and Luc Segoufin. Towards a characterization of order-invariant queries over tame structures. *Journal of Symbolic Logic*, 74(1):168–186, March 2009.

(RI-123) Susanna Donatelli, Serge Haddad, and Jeremy Sproston. Model checking timed and stochastic properties with CSL^{TA}. *IEEE Transactions on Software Engineering*, 35(2):224–240, March-April 2009.

(RI-124) Rémy Chevallier, Emmanuelle Encrenaz-Tiphène, Laurent Fribourg, and Weiwen Xu. Timed verification of the generic architecture of a memory circuit using parametric timed automata. *Formal Methods in System Design*, 34(1):59–81, February 2009.

(RI-125) Véronique Cortier and Stéphanie Delaune. Safely composing security protocols. *Formal Methods in System Design*, 34(1):1–36, February 2009.

(RI-126) Benedikt Bollig. On the expressive power of 2-stack visibly pushdown automata. *Logical Methods in Computer Science*, 4(4:16), December 2008.

(RI-127) Martin De Wulf, Laurent Doyen, Nicolas Markey, and Jean-François Raskin. Robust safety of timed automata. *Formal Methods in System Design*, 33(1-3):45–84, December 2008.

(RI-128) Stéphane Demri and Régis Gascon. Verification of qualitative $\mathbb{Z}$ constraints. *Theoretical Computer Science*, 409(1):24–40, December 2008.

(RI-129) Jean Goubault-Larrecq, Sławomir Lasota, and David Nowak. Logical relations for monadic types. *Mathematical Structures in Computer Science*, 18(6):1169–1217, December 2008. 81 pages.

(RI-130) Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Laure Petrucci. FAST : Acceleration from theory to practice. *International Journal on Software Tools for Technology Transfer*, 10(5):401–424, October 2008.

(RI-131) Yohan Boichut, Pierre-Cyrille Héam, and Olga Kouchnarenko. Approximation-based tree regular model-checking. *Nordic Journal of Computing*, 14(3):216–241, October 2008.

(RI-132) Sidney Rosario, Albert Benveniste, Stefan Haar, and Claude Jard. Probabilistic QoS and soft contracts for transaction-based web services orchestrations. *IEEE Transactions on Services Computing*, 1(4):187–200, October-December 2008.

(RI-133) Béatrice Bérard, Franck Cassez, Serge Haddad, Didier Lime, and Olivier H. Roux. When are timed automata weakly timed bisimilar to time Petri nets ? *Theoretical Computer Science*, 403(2-3):202–220, September 2008.

(RI-134) Benedikt Bollig and Dietrich Kuske. Muller message-passing automata and logics. *Information and Computation*, 206(9-10):1084–1094, September-October 2008.

(RI-135) Étienne Lozes, Daniel Hirschkoff, and Davide Sangiorgi. Separability in the ambient logic. *Logical Methods in Computer Science*, 4(3 :4), September 2008.

(RI-136) Serge Abiteboul, Omar Benjelloun, and Tova Milo. The active XML project : an overview. *The VLDB Journal*, 17(5):1019–1040, August 2008.

(RI-137) Patricia Bouyer, Kim G. Larsen, and Nicolas Markey. Model checking one-clock priced timed automata. *Logical Methods in Computer Science*, 4(2:9), June 2008.

(RI-138) Hubert Comon-Lundh, Florent Jacquemard, and Nicolas Perrin. Visibly tree automata with memory and constraints. *Logical Methods in Computer Science*, 4(2:8), June 2008.

(RI-139) Volker Diekert, Paul Gastin, and Manfred Kufleitner. A survey on small fragments of first-order logic over finite words. *International Journal of Foundations of Computer Science*, 19(3):513–548, June 2008.

(RI-140) Manfred Droste and Paul Gastin. On aperiodic and star-free formal power series in partially commuting variables. *Theory of Computing Systems*, 42(4):608–631, May 2008.

(RI-141) François Laroussinie, Nicolas Markey, and Ghassan Oreiby. On the expressiveness and complexity of ATL. *Logical Methods in Computer Science*, 4(2:7), May 2008.

(RI-142) Florent Jacquemard, Michaël Rusinowitch, and Laurent Vigneron. Tree automata with equality constraints modulo equational theories. *Journal of Logic and Algebraic Programming*, 75(2):182–208, April 2008.

(RI-143) Patricia Bouyer, Ed Brinksma, and Kim G. Larsen. Optimal infinite scheduling for multi-priced timed automata. *Formal Methods in System Design*, 32(1):2–23, February 2008.

(RI-144) Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis for monoidal equational theories. *Information and Computation*, 206(2-4):312–351, February-April 2008.

(RI-145) Panos Papadimitratos, Marcin Poturalski, Patrick Schaller, Pascal Lafourcade, David Basin, Srdjan Čapkun, and Jean-Pierre Hubaux. Secure neighborhood discovery : A fundamental element for mobile ad hoc networking. *IEEE Communications Magazine*, 46(2):132–139, February 2008.

(RI-146) Patricia Bouyer, Serge Haddad, and Pierre-Alain Reynier. Timed Petri nets and timed automata : On the discriminating power of Zeno sequences. *Information and Computation*, 206(1):73–107, January 2008.

(RI-147) Sami Taktak, Emmanuelle Encrenaz, and Jean-Lou Desbarbieux. A tool for automatic detection of deadlocks in wormhole networks on chip. *ACM Transactions on Design Automation of Electronic Systems*, 13(1), January 2008.

Articles dans d'autres revues

(RE-1) Pierre Senellart, Serge Abiteboul, and Rémi Gilleron. Understanding the hidden web. *ERCIM News*, 72:32–33, January 2008.

Communications invitées dans une conférence internationale

(IN-1) Elvio Gilberto Amparore, Benoît Barbot, Marco Beccuti, Susanna Donatelli, and Giuliana Franceschinis. Simulation-based verification of hybrid automata stochastic logic formulas for stochastic symmetric nets. *In* Gabriel A. Wainer, editor, *Proceedings of the 1st ACM SIGSIM Conference on Principles of Advanced Discrete Simulation (PADS'13), Montreal, Canada, May 2013*, pages 253–264. ACM Press.

(IN-2) Serge Abiteboul. Sharing distributed knowledge on the web (invited talk). *In* Patrick Cégielski and Arnaud Durand, editors, *Proceedings of the 21st Annual EACSL Conference on Computer Science Logic (CSL'12), Fontainebleau, France, September 2012*, volume 16 of *Leibniz International Proceedings in Informatics*, pages 6–8. Leibniz-Zentrum für Informatik.

(IN-3) Paul Gastin and Benjamin Monmege. Adding pebbles to weighted automata. *In* Nelma Moreira and Rogério Reis, editors, *Proceedings of the 17th International Conference on Implementation and Application of Automata (CIAA'12), Porto, Portugal, July 2012*, volume 7381 of *Lecture Notes in Computer Science*, pages 28–51. Springer-Verlag.

(IN-4) Serge Abiteboul. Viewing the web as a distributed knowledge base. *In* Yevgeny Kazakov, Domenico Lembo, and Frank Wolter, editors, *Proceedings of the 2012 International Workshop Description Logic (DL'09), Rome, Italy, June 2012*, volume 846 of *CEUR Workshop Proceedings*. RWTH Aachen, Germany.

(IN-5) Alain Finkel and Jean Goubault-Larrecq. The theory of WSTS : The case of complete WSTS. *In* Serge Haddad and Lucia Pomello, editors, *Proceedings of the 33rd International Conference on Applications and Theory of Petri Nets (ICATPN'12), Hamburg, Germany, June 2012*, volume 7347 of *Lecture Notes in Computer Science*, pages 3–31. Springer.

(IN-6) Serge Abiteboul, Émilien Antoine, and Julia Stoyanovich. Viewing the web as a distributed knowledge base. *In* Anastasios Kementsietsidis and Marcos Antonio Vaz Salles, editors, *Proceedings of the 28th International Conference on Data Engineering (ICDE'12), Washington, D.C., USA, April 2012*, pages 1–4. IEEE Computer Society Press.

(IN-7) Stefan Schwoon and César Rodríguez. Construction and SAT-based verification of contextual unfoldings. *In* Markus Holzer, Martin Kutrib, and Giovanni Pighizzini, editors, *Proceedings of the 13th International Workshop on Descriptional Complexity of Formal Systems (DCFS'11), Limburg, Germany, July 2011*, volume 6808 of *Lecture Notes in Computer Science*, pages 34–42. Springer.

(IN-8) Nicolas Markey. Robustness in real-time systems. *In Proceedings of the 6th IEEE International Symposium on Industrial Embedded Systems (SIES'11), Västerås, Sweden, June 2011*, pages 28–34. IEEE Computer Society Press.

(IN-9) Hubert Comon-Lundh and Véronique Cortier. How to prove security of communication protocols ? a discussion on the soundness of formal models w.r.t. computational ones. *In* Christoph Dürr and Thomas Schwentick, editors, *Proceedings of the 28th Annual Symposium on Theoretical Aspects of Computer Science (STACS'11), Dortmund, Germany, March 2011*, volume 9 of *Leibniz International Proceedings in Informatics*, pages 29–44. Leibniz-Zentrum für Informatik.

(IN-10) Krishnendu Chatterjee and Laurent Doyen. The complexity of partial-observation parity games. *In* Chrisaitn G. Fernmüller and Andrei Voronkov, editors, *Proceedings of the 17th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'10), Yogyakarta, Indonesia, October 2010*, volume 6397 of *Lecture Notes in Artificial Intelligence*, pages 1–14. Springer.

(IN-11) Stéphane Demri. Counter systems for data logics. *In* Ilkka Niemelä and Tomi Janhunen, editors, *Proceedings of the 12th European Conference on Logics in Artificial Intelligence (JELIA'10), Helsinki, Finland, September 2010*, volume 6431 of *Lecture Notes in Artificial Intelligence*, page 10. Springer.

(IN-12) Philippe Schnoebelen. Lossy counter machines decidability cheat sheet. *In* Antonín Kučera and Igor Potapov, editors, *Proceedings of the 4th Workshop on Reachability Problems in Computational Models (RP'10), Brno, Czech Republic, August 2010*, volume 6227 of *Lecture Notes in Computer Science*, pages 51–75. Springer.

(IN-13) Jean Goubault-Larrecq. Noetherian spaces in verification. *In* Samson Abramsky, Friedhelm Meyer auf der Heide, and Paul Spirakis, editors, *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP'10) – Part II, Bordeaux, France, July 2010*, volume 6199 of *Lecture Notes in Computer Science*, pages 2–21. Springer.

(IN-14) Laurent Doyen and Jean-François Raskin. Antichains algorithms for finite automata. *In* Javier Esparza and Rupak Majumdar, editors, *Proceedings of the 16th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'10), Paphos, Cyprus, March 2010*, volume 6015 of *Lecture Notes in Computer Science*, pages 2–22. Springer.

(IN-15) Jean Goubault-Larrecq. "Logic wins !". *In* Anupam Datta, editor, *Proceedings of the 13th Asian Computing Science Conference (ASIAN'09), Seoul, Korea, December 2009*, volume 5913 of *Lecture Notes in Computer Science*, pages 1–16. Springer.

(IN-16) Serge Abiteboul, Pierre Bourhis, Alban Galland, and Bogdan Marinoiu. The AXML artifact model. *In Proceedings of the 16th International Symposium on Temporal Representation and Reasoning (TIME'09), Brixen-Bressanone, Italy, July 2009*, pages 11–17. IEEE Computer Society Press.

(IN-17) Martín Abadi, Bruno Blanchet, and Hubert Comon-Lundh. Models and proofs of protocol security : A progress report. *In* Ahmad Bouajjani and Oded Maler, editors, *Proceedings of the 21st International Conference on Computer Aided Verification (CAV'09), Grenoble, France, June-July 2009*, volume 5643 of *Lecture Notes in Computer Science*, pages 35–49. Springer.

(IN-18) Benedikt Bollig and Paul Gastin. Weighted versus probabilistic logics. *In* Volker Diekert and Dirk Nowotka, editors, *Proceedings of the 13th International Conference on Developments in Language Theory (DLT'09), Stuttgart, Germany, June-July 2009*, volume 5583 of *Lecture Notes in Computer Science*, pages 18–38. Springer.

(IN-19) Patricia Bouyer. Model-checking timed temporal logics. *In* Carlos Areces and Stéphane Demri, editors, *Proceedings of the 4th Workshop on Methods for Modalities (M4M-5), Cachan, France, November 2007*, volume 231 of *Electronic Notes in Theoretical Computer Science*, pages 323–341. Elsevier Science Publishers, March 2009.

(IN-20) Steve Kremer. Computational soundness of equational theories (tutorial). *In* Gilles Barthe and Cédric Fournet, editors, *Revised Selected Papers from the 3rd Symposium on Trustworthy Global Computing (TGC'07), Sophia-Antipolis, France, November 2007*, volume 4912 of *Lecture Notes in Computer Science*, pages 363–382. Springer, 2008.

(IN-21) Hubert Comon-Lundh. About models of security protocols. *In* Ramesh Hariharan, Madhavan Mukund, and V. Vinay, editors, *Proceedings of the 28th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'08), Bangalore, India, December 2008*, volume 2 of *Leibniz International Proceedings in Informatics*. Leibniz-Zentrum für Informatik.

(IN-22) Hubert Comon-Lundh. Challenges in the automated verification of security protocols. *In* Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *Proceedings of the 4th International Joint Conference on Automated Reasoning (IJCAR'08), Sydney, Australia, August 2008*, volume 5195 of *Lecture Notes in Artificial Intelligence*, pages 396–409. Springer-Verlag.

(IN-23) Jean Goubault-Larrecq and Julien Olivain. A smell of orchids. *In* Martin Leucker, editor, *Proceedings of the 8th Workshop on Runtime Verification (RV'08), Budapest, Hungary, March 2008*, volume 5289 of *Lecture Notes in Computer Science*, pages 1–20. Springer.

Autres communications sur invitation, tutorials, ...

(In-1) Laurent Fribourg. En quoi Turing a-t-il changé ma vie ?, April 2012.

(In-2) Jean Goubault-Larrecq. A few pearls in the theory of quasi-metric spaces. Invited talk, Fifth International Conference on Topology, Algebra, and Categories in Logic (TACL'11), Marseilles, France, July 2011, July 2011.

(In-3) Leonid Libkin and Cristina Sirangelo. Open and closed world assumptions in data exchange. *In* Bernardo Cuenca Grau, Ian Horrocks, Boris Motik, and Ulrike Sattler, editors, *Proceedings of the 22nd International Workshop Description Logic (DL'09), Oxford, UK, July 2009*, volume 477 of *CEUR Workshop Proceedings*, pages 1–6. RWTH Aachen, Germany.

(In-4) Patricia Bouyer. Probabilities in timed automata. Invited talk, Workshop Automata and Verification (AV'08), Mons, Belgium, August 2008.

(In-5) Nicolas Markey. Infinite runs in weighted times games with energy constraints. Invited talk, Workshop Automata and Verification (AV'08), Mons, Belgium, August 2008.

(In-6) Philippe Schnoebelen. The complexity of lossy channel systems. Invited talk, Workshop Automata and Verification (AV'08), Mons, Belgium, August 2008.

(In-7) Nicolas Markey. Timed systems – model checking and games. Invited tutorial, 8th School on Modelling and Verifying Parallel Processes (MOVEP'08), Nouan-le-Fuzelier, France, June 2008.

(In-8) Patricia Bouyer. Model-checking timed temporal logics. *In* Tei-Wei Kuo and Samuel Cruz-Lara, editors, *Proceedings of the 4th Taiwanese-French Conference on Information Technology (TFIT'08), Taipei, Taiwan, March 2008*, pages 132–142.

(In-9) Stéphanie Delaune, Steve Kremer, and Graham Steel. Formal analysis of PKCS#11. *In* Tei-Wei Kuo and Samuel Cruz-Lara, editors, *Proceedings of the 4th Taiwanese-French Conference on Information Technology (TFIT'08), Taipei, Taiwan, March 2008*, pages 267–278.

Communications dans des conférences internationales avec comité de lecture

(CI-1) Assalé Adjé, Olivier Bouissou, Jean Goubault-Larrecq, Éric Goubault, and Sylvie Putot. Analyzing numerical programs with partially known distributions. *In* Ernie Cohen and Andrey Rybalchenko, editors, *Preliminary Proceedings of the 5th IFIP TC2/WG2.3 Conference Verified Software—Theories, Tools, and Experiments (VSTTE'13), Atherton, California, USA, May 2013*, Lecture Notes in Computer Science. Springer, 2013.

(CI-2) Serge Abiteboul and Victor Vianu. Collaborative data-driven workflows : Think global, act local. *In* Wenfei Fan, editor, *Proceedings of the 32nd Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'13), New York, New York, USA, June 2013*, pages 91–102. ACM Press.

(CI-3) Arjun Arul and Julien Reichert. The complexity of robot games on the integer line. *In* Luca Bortolussi and Herbert Wiklicky, editors, *Proceedings of the 11th International Workshop on Quantitative Aspects of Programming Languages (QAPI'13), Rome, Italy, June 2013*, volume 117 of *Electronic Proceedings in Theoretical Computer Science*, pages 132–148.

(CI-4) Nathalie Bertrand and Philippe Schnoebelen. Solving stochastic büchi games on infinite arenas with a finite attractor. *In* Luca Bortolussi and Herbert Wiklicky, editors, *Proceedings of the 11th International Workshop on Quantitative Aspects of Programming Languages (QAPI'13), Rome, Italy, June 2013*, volume 117 of *Electronic Proceedings in Theoretical Computer Science*, pages 116–131.

(CI-5) Mikołaj Bojańczyk, Luc Segoufin, and Szymon Toruńczyk. Verification of database-driven systems via amalgamation. *In* Wenfei Fan, editor, *Proceedings of the 32nd Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'13), New York, New York, USA, June 2013*, pages 63–74. ACM Press.

(CI-6) Benedikt Bollig, Peter Habermehl, Martin Leucker, and Benjamin Monmege. A fresh approach to learning register automata. *In* Marie-Pierre Béal and Olivier Carton, editors, *Proceedings of the 17th International Conference on Developments in Language Theory (DLT'13), Marne-la-Vallée, France, June 2013*, volume 7907 of *Lecture Notes in Computer Science*, pages 118–130. Springer.

(CI-7) Benedikt Bollig, Dietrich Kuske, and Roy Mennicke. The complexity of model checking multi-stack systems. *In Proceedings of the 28th Annual IEEE Symposium on Logic in Computer Science (LICS'13), New-Orleans, Louisiana, USA, June 2013*, pages 163–170. IEEE Computer Society Press.

(CI-8) Anudhyan Boral and Sylvain Schmitz. Model checking parse trees. *In Proceedings of the 28th Annual IEEE Symposium on Logic in Computer Science (LICS'13), New-Orleans, Louisiana, USA, June 2013*, pages 153–162. IEEE Computer Society Press.

(CI-9) Thomas Chatain and Stefan Haar. A canonical contraction for safe Petri nets. *In* Daniel Moldt and Heiko Rölke, editors, *Proceedings of the 7th International Workshop on Petri Nets and Software Engineering (PNSE'13), Milano, Italy, June 2013*, volume 969 of *CEUR Workshop Proceedings*, pages 25–39. RWTH Aachen, Germany.

(CI-10) Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. Tractable inference systems : an extension with a deducibility predicate. *In* Maria Paola Bonacina, editor, *Proceedings of the 24th International Conference on Automated Deduction (CADE'13), Lake Placid, New York, USA, June 2013*, volume 7898 of *Lecture Notes in Artificial Intelligence*, pages 91–108. Springer.

(CI-11) Stéphane Demri, Diego Figueira, and M. Praveen. Reasoning about data repetitions with counter systems. *In Proceedings of the 28th Annual IEEE Symposium on Logic in Computer Science (LICS'13), New-Orleans, Louisiana, USA, June 2013*, pages 33–42. IEEE Computer Society Press.

(CI-12) Estíbaliz Fraca and Serge Haddad. Complexity analysis of continuous Petri nets. *In* José-Manuel Colom and Jörg Desel, editors, *Proceedings of the 34th International Conference on Applications and Theory of Petri Nets (ICATPN'13), Milano, Italy, June 2013*, volume 7927 of *Lecture Notes in Computer Science*, pages 170–189. Springer.

(CI-13) Gilles Geeraerts, Alexander Heußner, M. Praveen, and Jean-François Raskin. ω-Petri nets. *In* José-Manuel Colom and Jörg Desel, editors, *Proceedings of the 34th International Conference on Applications and Theory of Petri Nets (ICATPN'13), Milano, Italy, June 2013*, volume 7927 of *Lecture Notes in Computer Science*, pages 49–69. Springer.

(CI-14) Amélie Gheerbrant, Leonid Libkin, and Cristina Sirangelo. When is naïve evaluation possible ? *In* Wenfei Fan, editor, *Proceedings of the 32nd Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'13), New York, New York, USA, June 2013*, pages 75–86. ACM Press.

(CI-15) Serge Haddad, Rolf Hennicker, and Mikael H. Møller. Channel properties of asynchronously composed Petri nets. *In* José-Manuel Colom and Jörg Desel, editors, *Proceedings of the 34th International Conference on Applications and Theory of Petri Nets (ICATPN'13), Milano, Italy, June 2013*, volume 7927 of *Lecture Notes in Computer Science*, pages 369–388. Springer.

(CI-16) Wojciech Kazana and Luc Segoufin. Enumeration of first-order queries on classes of structures with bounded expansion. *In* Wenfei Fan, editor, *Proceedings of the 32nd Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'13), New York, New York, USA, June 2013*, pages 297–308. ACM Press.

(CI-17) César Rodríguez, Stefan Schwoon, and Victor Khomenko. Contextual merged processes. *In* José-Manuel Colom and Jörg Desel, editors, *Proceedings of the 34th International Conference on Applications and Theory of Petri Nets (ICATPN'13), Milano, Italy, June 2013*, volume 7927 of *Lecture Notes in Computer Science*, pages 29–48. Springer.

(CI-18) Benedikt Bollig, Aiswarya Cyriac, Loïc Hélouët, Ahmet Kara, and Thomas Schwentick. Dynamic communicating automata and branching high-level MSCs. *In* Adrian Horia Dediu, Carlos Martín-Vide, and Bianca Truthe, editors, *Proceedings of the 7th International Conference on Language and Automata Theory and Applications (LATA'13), Bilbao, Spain, April 2013*, volume 7810 of *Lecture Notes in Computer Science*, pages 177–189. Springer.

(CI-19) Serge Abiteboul, Pierre Bourhis, Anca Muscholl, and Zhilin Wu. Recursive queries on trees and data trees. *In* Wang-Chiew Tan, Giovanna Guerrini, Barbara Catania, and Anastasios Gounaris, editors, *Proceedings of the 16th International Conference on Database Theory (ICDT'13), Genoa, Italy, March 2013*, pages 93–104. ACM Press.

(CI-20) Eberhard Bertsch, Mark-Jan Nederhof, and Sylvain Schmitz. On LR parsing with selective delays. *In* Koen De Bosschere and Ranjit Jhala, editors, *Proceedings of the 22nd International Conference on Compiler Construction (CC'13), Rome, Italy, March 2013*, volume 7791 of *Lecture Notes in Computer Science*, pages 244–263. Springer.

(CI-21) Benedikt Bollig, Paul Gastin, and Benjamin Monmege. Weighted specifications over nested words. *In* Frank Pfenning, editor, *Proceedings of the 16th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'13), Rome, Italy, March 2013*, volume 7794 of *Lecture Notes in Computer Science*, pages 385–400. Springer.

(CI-22) Vincent Cheval and Bruno Blanchet. Proving more observational equivalences with proverif. *In* David Basin and John Mitchell, editors, *Proceedings of the 2nd International Conference on Principles of Security and Trust (POST'13, Rome, Italy, March 2013*, Lecture Notes in Computer Science, pages 226–246. Springer.

(CI-23) Rémy Chrétien and Stéphanie Delaune. Formal analysis of privacy for routing protocols in mobile ad hoc networks. *In* David Basin and John Mitchell, editors, *Proceedings of the 2nd International Conference on Principles of Security and Trust (POST'13, Rome, Italy, March 2013*, Lecture Notes in Computer Science, pages 1–20. Springer.

(CI-24) Prateek Karandikar and Sylvain Schmitz. The parametric ordinal-recursive complexity of Post embedding problems. *In* Frank Pfenning, editor, *Proceedings of the 16th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'13), Rome, Italy, March 2013*, volume 7794 of *Lecture Notes in Computer Science*, pages 273–288. Springer.

(CI-25) Pedro Cabalar and Stéphane Demri. Automata-based computation of temporal equilibrium models. *In* Germán Vidal, editor, *Proceedings of the 21st International Workshop on Logic Program Synthesis and Transformation (LOPSTR'11), Odense, Denmark, July 2011*, volume 7225 of *Lecture Notes in Computer Science*, pages 57–72. Springer, 2012.

(CI-26) Étienne Lozes and Jules Villard. Reliable contracts for unreliable half-duplex communications. *In* Marco Carbone and Jean-Marc Petit, editors, *Revised Selected Papers of the 8th International Workshop on Web Services and Formal Methods (WS-FM'11), Clermont-Ferrand, France, September 2011*, volume 7176 of *Lecture Notes in Computer Science*, pages 2–16. Springer, 2012.

(CI-27) Rémi Bonnet, Alain Finkel, and M. Praveen. Extending the Rackoff technique to affine nets. *In* Deepak D'Souza, Jaikumar Radhakrishnan, and Kavitha Telikepalli, editors, *Proceedings of the 32nd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'12), Hyderabad, India, December 2012*, Leibniz International Proceedings in Informatics. Leibniz-Zentrum für Informatik.

(CI-28) Ana Bušić, Hilal Djafri, and Jean-Michel Fourneau. Bounded state space truncation and censored Markov chains. *In Proceedings of the 51st IEEE Conference on Decision and Control (CDC'12), Maui, Hawaii, USA, December 2012*, pages 5828–5833. IEEE Control System Society.

(CI-29) Benoît Barbot, Serge Haddad, and Claudine Picaronny. Importance sampling for model checking of continuous time Markov chains. *In* Petre Dini and Pascal Lorenz, editors, *Proceedings of the 4th International Conference on Advances in System Simulation (SIMUL'12), Lisbon, Portugal, November 2012*, pages 30–35. XPS.

(CI-30) Benedikt Bollig, Paul Gastin, Benjamin Monmege, and Marc Zeitoun. A probabilistic Kleene theorem. *In* Madhavan Mukund and Supratik Chakraborty, editors, *Proceedings of the 10th International Symposium on Automated Technology for Verification and Analysis (ATVA'12), Thiruvananthapuram, India, October 2012*, volume 7561 of *Lecture Notes in Computer Science*, pages 400–415. Springer.

(CI-31) Sandie Balaguer and Thomas Chatain. Avoiding shared clocks in networks of timed automata. *In* Maciej Koutny and Irek Ulidowski, editors, *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR'12), Newcastle, UK, September 2012*, volume 7454 of *Lecture Notes in Computer Science*, pages 100–114. Springer.

(CI-32) Béatrice Bérard, Serge Haddad, Mathieu Sassolas, and Nathalie Sznajder. Concurrent games on VASS with inhibition. *In* Maciej Koutny and Irek Ulidowski, editors, *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR'12), Newcastle, UK, September 2012*, volume 7454 of *Lecture Notes in Computer Science*, pages 39–52. Springer.

(CI-33) Patricia Bouyer, Thomas Brihaye, Marcin Jurdziński, and Quentin Menet. Almost-sure model-checking of reactive timed automata. *In Proceedings of the 9th International Conference on Quantitative Evaluation of Systems (QEST'12), London, UK, September 2012*, pages 138–147. IEEE Computer Society Press.

(CI-34) Patricia Bouyer, Kim G. Larsen, and Nicolas Markey. Lower-bound constrained runs in weighted timed automata. *In Proceedings of the 9th International Conference on Quantitative Evaluation of Systems (QEST'12), London, UK, September 2012*, pages 128–137. IEEE Computer Society Press.

(CI-35) Romain Brenguier, Stefan Göller, and Ocan Sankur. A comparison of succinctly represented finite-state systems. *In* Maciej Koutny and Irek Ulidowski, editors, *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR'12), Newcastle, UK, September 2012*, volume 7454 of *Lecture Notes in Computer Science*, pages 147–161. Springer.

(CI-36) Aiswarya Cyriac, Paul Gastin, and K. Narayan Kumar. MSO decidability of multi-pushdown systems via split-width. *In* Maciej Koutny and Irek Ulidowski, editors, *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR'12), Newcastle, UK, September 2012*, volume 7454 of *Lecture Notes in Computer Science*, pages 547–561. Springer.

(CI-37) Arnaud Da Costa, François Laroussinie, and Nicolas Markey. Quantified CTL : expressiveness and model checking. *In* Maciej Koutny and Irek Ulidowski, editors, *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR'12), Newcastle, UK, September 2012*, volume 7454 of *Lecture Notes in Computer Science*, pages 177–192. Springer.

(CI-38) Laurent Fribourg, David Lesens, Pierre Moro, and Romain Soulat. Robustness analysis for scheduling problems using the inverse method. *In* Mark Reynolds, Paolo Terenziani, and Ben Moszkowski, editors, *Proceedings of the 19th International Symposium on Temporal Representation and Reasoning (TIME'12), Leicester, UK, September 2012*, pages 73–80. IEEE Computer Society Press.

(CI-39) Petr Jančar, Prateek Karandikar, and Philippe Schnoebelen. Unidirectional channel systems can be tested. *In* Jos Baeten, Tom Ball, and Frank de Boer, editors, *Proceedings of the 7th IFIP International Conference on Theoretical Computer Science (TCS'12), Amsterdam, The Netherlands, September 2012*, volume 7604 of *Lecture Notes in Computer Science*, pages 149–163. Springer.

(CI-40) Robert Künnemann and Graham Steel. YubiSecure ? formal security analysis results for the Yubikey and YubiHSM. *In* Audun Jøsang, Pierangela Samarati, and Marinella Petrocchi, editors, *Revised Selected Papers of the 8th Workshop on Security and Trust Management (STM'12), Pisa, Italy, September 2012*, volume 7783 of *Lecture Notes in Computer Science*, pages 257–272. Springer.

(CI-41) César Rodríguez and Stefan Schwoon. Verification of Petri nets with read arcs. *In* Maciej Koutny and Irek Ulidowski, editors, *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR'12), Newcastle, UK, September 2012*, volume 7454 of *Lecture Notes in Computer Science*, pages 471–485. Springer.

(CI-42) Anoopam Agarwal, Agnes Madalinski, and Stefan Haar. Effective verification of weak diagnosability. *In Proceedings of the 8th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS'12), Mexico City, Mexico, August 2012*. IFAC.

(CI-43) Étienne André, Laurent Fribourg, Ulrich Kühne, and Romain Soulat. IMITATOR 2.5 : A tool for analyzing robustness in scheduling problems. *In* Dimitra Giannakopoulou and Dominique Méry, editors, *Proceedings of the 18th International Symposium on Formal Methods (FM'12), Paris, France, August 2012*, volume 7436 of *Lecture Notes in Computer Science*, pages 33–36. Springer.

(CI-44) Romain Bardou, Riccardo Focardi, Yusuke Kawamoto, Lorenzo Simionato, Graham Steel, and Joe-Kai Tsay. Efficient padding oracle attacks on cryptographic hardware. *In* Reihaneh Safavi-Naini and Ran Canetti, editors, *Proceedings of the 32nd Annual International Cryptology Conference (CRYPTO'12), Santa Barbara, California, USA, August 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 608–625. Springer.

(CI-45) Dietmar Berwanger, Łukasz Kaiser, and Simon Leßenich. Solving counter parity games. *In* Branislav Rovan, Vladimiro Sassone, and Peter Widmayer, editors, *Proceedings of the 37th International Symposium on Mathematical Foundations of Computer Science (MFCS'12), Bratislava, Slovakia, August 2012*, volume 7464 of *Lecture Notes in Computer Science*, pages 160–171. Springer.

(CI-46) Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. Unambiguous constrained automata. *In* Hsu-Chun Yen and Oscar H. Ibarra, editors, *Proceedings of the 16th International Conference on Developments in Language Theory (DLT'12), Taipei, Taiwan, August 2012*, volume 7410 of *Lecture Notes in Computer Science*, pages 239–250. Springer.

(CI-47) Facundo Carreiro and Stéphane Demri. Beyond regularity for Presburger modal logics. *In* Thomas Bolander, Torben Braüner, Silvio Ghilardi, and Lawrence Moss, editors, *Selected Papers from the 9th Workshop on Advances in Modal Logics (AiML'12), Copenhagen, Denmark, August 2012*, pages 161–182. College Publications.

(CI-48) Hedi Benzina. A network policy model for virtualized systems. *In Proceedings of the 17th IEEE Symposium on Computers and Communications (ISCC'12), Nevşehir, Turkey, July 2012*, pages 680–683. IEEE Computer Society Press.

(CI-49) Benedikt Bollig, Normann Decker, and Martin Leucker. Frequency linear-time temporal logic. *In Proceedings of the 6th International Symposium on Theoretical Aspects of Software Engineering (TASE'12), Beijing, China, July 2012*, pages 85–92. IEEE Computer Society Press.

(CI-50) Patricia Bouyer, Nicolas Markey, and Ocan Sankur. Robust reachability in timed automata : A game-based approach. *In* Artur Czumaj, Kurt Mehlhorn, Andrew Pitts, and Roger Wattenhofer, editors, *Proceedings of the 39th International Colloquium on Automata, Languages and Programming (ICALP'12) – Part II, Warwick, UK, July 2012*, volume 7392 of *Lecture Notes in Computer Science*, pages 128–140. Springer.

(CI-51) Prateek Karandikar and Philippe Schnoebelen. Cutting through regular Post embedding problems. *In* Edward A. Hirsch, Juhani Karhumäki, Arto Lepistö, and Michail Prilutskii, editors, *Proceedings of the 7th International Computer Science Symposium in Russia (CSR'12), Nizhni Novgorod, Russia, July 2012*, volume 7353 of *Lecture Notes in Computer Science*, pages 229–240. Springer.

(CI-52) Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune. Verifying privacy-type properties in a modular way. *In Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF'12), Cambridge Massachusetts, USA, June 2012*, pages 95–109. IEEE Computer Society Press.

(CI-53) Krishnendu Chatterjee and Laurent Doyen. Partial-observation stochastic games : How to win when belief fails. *In Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science (LICS'12), Dubrovnik, Croatia, June 2012*, pages 175–184. IEEE Computer Society Press.

(CI-54) Stéphanie Delaune, Steve Kremer, and Daniel Pasailă. Security protocols, constraint systems, and group theories. *In* Bernhard Gramlich, Dale Miller, and Uli Sattler, editors, *Proceedings of the 6th International Joint Conference on Automated Reasoning (IJCAR'12), Manchester, UK, June 2012*, volume 7364 of *Lecture Notes in Artificial Intelligence*, pages 164–178. Springer-Verlag.

(CI-55) Stéphane Demri, Amit Kumar Dhar, and Arnaud Sangnier. Taming past LTL and flat counter systems. *In* Bernhard Gramlich, Dale Miller, and Uli Sattler, editors, *Proceedings of the 6th International Joint Conference on Automated Reasoning (IJCAR'12), Manchester, UK, June 2012*, volume 7364 of *Lecture Notes in Artificial Intelligence*, pages 179–193. Springer-Verlag.

(CI-56) Serge Haddad, Sylvain Schmitz, and Philippe Schnoebelen. The ordinal-recursive complexity of timed-arc Petri nets, data nets, and other enriched nets. *In Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science (LICS'12), Dubrovnik, Croatia, June 2012*, pages 355–364. IEEE Computer Society Press.

(CI-57) Serge Abiteboul, Yael Amsterdamer, Tova Milo, and Pierre Senellart. Auto-completion learning for XML. *In* K. Selçuk Candan, Yi Chen, Richard T. Snodgrass, Luis Gravano, and Ariel Fuxman, editors, *Proceedings of the ACM SIGMOD Internaitonal Conference on Management of Data (SIGMOD'12), Scottsdale, Arizona, USA, May 2012*, pages 669–672. ACM Press.

(CI-58) Hedi Benzina. Towards designing secure virtualized systems. *In Proceedings of the 2nd International Conference on Digital Information and Communication Technology and its Application (DICTAP'12), Bangkok, Thailand, May 2012*, pages 250–255. IEEE Computer Society Press.

(CI-59) Malika Izabachène and Benoît Libert. Divisible e-cash in the standard model. *In* Michel Abdalla and Tanja Lange, editors, *Proceedings of the 5th International Conference on Pairing-Based Cryptography (PAIRING'12), Cologne, Germany, May 2012*, volume 7708 of *Lecture Notes in Computer Science*, pages 314–332. Springer.

(CI-60) Hernán Ponce de León, Stefan Haar, and Delphine Longuet. Conformance relations for labeled event structures. *In* Achim D. Brucker and Jacques Julliand, editors, *Proceedings of the 6th International Conference on Tests and Proofs (TAP'12), Prague, Czech Republic, May-June 2012*, volume 7305 of *Lecture Notes in Computer Science*, pages 83–98. Springer.

(CI-61) Abiteboul Serge, Meghyn Bienvenu, and Daniel Deutch. Deduction in the presence of distribution and contradictions. *In* Zachary G. Ives and Yannis Velegrakis, editors, *Proceedings of the 15th International Workshop on the Web and Databases (WebDB'12), Scottsdale, Arizona, USA, May 2012*, pages 31–36.

(CI-62) Serge Abiteboul, Pierre Senellart, and Victor Vianu. The ERC webdam on foundations of web data management. *In* Alain Mille, Fabien L. Gandon, Jacques Misselis, Michael Rabinovich, and Steffen Staab, editors, *Proceedings of the 21st World Wide Web Conference (WWW'12) – Companion Volume, Lyon, France, April 2012*, pages 211–214. ACM Press.

(CI-63) Étienne André, Laurent Fribourg, and Romain Soulat. Enhancing the inverse method with state merging. *In* Alwyn Goodloe and Suzette Person, editors, *Proceedings of the 4th NASA Formal Methods Symposium (NFM'12), Norfolk, Virginia, USA, April 2012*, volume 7226 of *Lecture Notes in Computer Science*, pages 100–105. Springer.

(CI-64) Serge Abiteboul, Yael Amsterdamer, Daniel Deutch, Tova Milo, and Pierre Senellart. Finding optimal probabilistic generators for XML collections. *In* Alin Deutsch, editor, *Proceedings of the 15th International Conference on Database Theory (ICDT'12), Berlin, Germany, March 2012*, pages 127–139. ACM Press.

(CI-65) Serge Abiteboul, Pierre Bourhis, and Victor Vianu. Highly expressive query languages for unordered data trees. *In* Alin Deutsch, editor, *Proceedings of the 15th International Conference on Database Theory (ICDT'12), Berlin, Germany, March 2012*, pages 46–60. ACM Press.

(CI-66) Gergei Bana and Hubert Comon-Lundh. Towards unconditional soundness : Computationally complete symbolic attacker. *In* Pierpaolo Degano and Joshua D. Guttman, editors, *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12), Tallinn, Estonia, March 2012*, volume 7215 of *Lecture Notes in Computer Science*, pages 189–208. Springer.

(CI-67) Benoît Barbot, Serge Haddad, and Claudine Picaronny. Coupling and importance sampling for statistical model checking. *In* Cormac Flanagan and Barbara König, editors, *Proceedings of the 18th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'12), Tallinn, Estonia, March 2012*, volume 7214 of *Lecture Notes in Computer Science*, pages 331–346. Springer.

(CI-68) Ghania Belkacem, Denis Labrousse, Stéphane Lefebvre, Pierre-Yves Joubert, Ulrich Kühne, Laurent Fribourg, Romain Soulat, Éric Florentin, and Christian Rey. Distributed and coupled electrothermal model of power semiconductor devices. *In* Rafik Neji, editor, *Proceedings of the 1st International Conference on Renewable Energies and VEhicular Technology (REVET'12), Hammamet, Tunisia, March 2012*, pages 84–89. IEEE Power & Energy Society.

(CI-69) Benedikt Bollig, Aiswarya Cyriac, Paul Gastin, and K. Narayan Kumar. Model checking languages of data words. *In* Lars Birkedal, editor, *Proceedings of the 15th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'12), Tallinn, Estonia, March 2012*, volume 7213 of *Lecture Notes in Computer Science*, pages 391–405. Springer.

(CI-70) Patricia Bouyer, Romain Brenguier, Nicolas Markey, and Michael Ummels. Concurrent games with ordered objectives. *In* Lars Birkedal, editor, *Proceedings of the 15th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'12), Tallinn, Estonia, March 2012*, volume 7213 of *Lecture Notes in Computer Science*, pages 301–315. Springer.

(CI-71) Rohit Chadha, Ştefan Ciobâcă, and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. *In* Helmut Seidl, editor, *Programming Languages and Systems — Proceedings of the 22nd European Symposium on Programming (ESOP'12), Tallinn, Estonia, March 2012*, volume 7211 of *Lecture Notes in Computer Science*, pages 108–127. Springer.

(CI-72) Rohit Chadha, P. Madhusudan, and Mahesh Viswanathan. Reachability under contextual locking. *In* Cormac Flanagan and Barbara König, editors, *Proceedings of the 18th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'12), Tallinn, Estonia, March 2012*, volume 7214 of *Lecture Notes in Computer Science*, pages 437–450. Springer.

(CI-73) Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. Security proof with dishonest keys. *In* Pierpaolo Degano and Joshua D. Guttman, editors, *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12), Tallinn, Estonia, March 2012*, volume 7215 of *Lecture Notes in Computer Science*, pages 149–168. Springer.

(CI-74) Véronique Cortier, Jan Degrieck, and Stéphanie Delaune. Analysing routing protocols : four nodes topologies are sufficient. *In* Pierpaolo Degano and Joshua D. Guttman, editors, *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12), Tallinn, Estonia, March 2012*, volume 7215 of *Lecture Notes in Computer Science*, pages 30–50. Springer.

(CI-75) Martin Lange and Étienne Lozes. Model-checking the higher-dimensional modal μ-calculus. *In* Dale Miller and Zoltán Ésik, editors, *Proceedings of the 8th Workshop on Fixed Points in Computer Science (FICS'12), Tallinn, Estonia, March 2012*, volume 77 of *Electronic Proceedings in Theoretical Computer Science*, pages 39–46.

(CI-76) Morten Dahl, Stéphanie Delaune, and Graham Steel. Formal analysis of privacy for anonymous location based services. *In* Sebastian A. Mödersheim and Catuscia Palamidessi, editors, *Revised Selected Papaers of the Workshop on Theory of Security and Applications (TOSCA'11), Saarbrücken, Germany, March-April 2011*, volume 6993 of *Lecture Notes in Computer Science*, pages 98–112. Springer, January 2012.

(CI-77) Florent Jacquemard, Étienne Lozes, Ralf Treinen, and Jules Villard. Multiple congruence relations, first-order theories on terms, and the frames of the applied pi-calculus. *In* Sebastian A. Mödersheim and Catuscia Palamidessi, editors, *Revised Selected Papaers of the Workshop on Theory of Security and Applications (TOSCA'11), Saarbrücken, Germany, March-April 2011*, volume 6993 of *Lecture Notes in Computer Science*, pages 166–185. Springer, January 2012.

(CI-78) Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, and Martin Leucker. SMA—the Smyle modeling approach. *In* Zbigniew Huzar, Radek Kocí, Bertrand Meyer, Bartosz Walter, and Jaroslav Zendulka, editors, *Revised Selected Papars of the 3rd IFIP TC2 Central and East European Conference on Software Engineering Techniques (CEE-SET'08), Brno, Czech Republic, October 2008*, volume 4980 of *Lecture Notes in Computer Science*, pages 103–117. Springer, 2011.

(CI-79) Dietmar Berwanger, Łukasz Kaiser, and Bernd Puchala. Perfect-information construction for coordination in games. *In* Supratik Chakraborty and Amit Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11), Mumbai, India, December 2011*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 387–398. Leibniz-Zentrum für Informatik.

(CI-80) Patricia Bouyer, Romain Brenguier, Nicolas Markey, and Michael Ummels. Nash equilibria in concurrent games with Büchi objectives. *In* Supratik Chakraborty and Amit Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11), Mumbai, India, December 2011*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 375–386. Leibniz-Zentrum für Informatik.

(CI-81) Céline Chevalier, Stéphanie Delaune, and Steve Kremer. Transforming password protocols to compose. *In* Supratik Chakraborty and Amit Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11), Mumbai, India, December 2011*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 204–216. Leibniz-Zentrum für Informatik.

(CI-82) Philippe Darondeau, Stéphane Demri, Roland Meyer, and Christophe Morvan. Petri net reachability graphs : Decidability status of FO properties. *In* Supratik Chakraborty and Amit Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11), Mumbai, India, December 2011*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 140–151. Leibniz-Zentrum für Informatik.

(CI-83) Malika Izabachène, Benoît Libert, and Damien Vergnaud. Block-wise P-signatures and non-interactive anonymous credentials with efficient attributes. *In* Liqun Chen, editor, *Proceedings of the 13th IMA International Conference on Cryptography and Coding (IMACC'11), Oxford, UK, December 2011*, volume 7089 of *Lecture Notes in Computer Science*, pages 431–450. Springer.

(CI-84) Ocan Sankur, Patricia Bouyer, and Nicolas Markey. Shrinking timed automata. *In* Supratik Chakraborty and Amit Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11), Mumbai, India, December 2011*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 90–102. Leibniz-Zentrum für Informatik.

(CI-85) Benoît Barbot, Serge Haddad, and Claudine Picaronny. Échantillonnage préférentiel pour le model checking statistique. *In* Étienne Craye and Abdoulaye Gamatié, editors, *Actes du 0ème Colloque sur la Modélisation des Systèmes Réactifs (MSR'11), Lille, France, November 2011*, volume 45(1-3) of *Journal Européen des Systèmes Automatisés*, pages 237–252. Hermès.

(CI-86) Jodé Echeveste, Arshia Cont, Jean-Louis Giavitto, and Florent Jacquemard. Formalisation des relations temporelles entre une partition et une performance musicale dans un contexte d'accompagnement automatique. *In* Étienne Craye and Abdoulaye Gamatié, editors, *Actes du 0ème Colloque sur la Modélisation des Systèmes Réactifs (MSR'11), Lille, France, November 2011*, volume 45(1-3) of *Journal Européen des Systèmes Automatisés*, pages 109–124. Hermès.

(CI-87) Marcello Bersani and Stéphane Demri. The complexity of reversal-bounded model-checking. *In* Cesare Tinelli and Viorica Sofronie-Stokkermans, editors, *Proceedings of the 8th International Symposium on Frontiers of Combining Systems (FroCoS'11), Saarbrücken, Germany, October 2011*, volume 6989 of *Lecture Notes in Artificial Intelligence*, pages 71–86. Springer.

(CI-88) Patricia Bouyer, Nicolas Markey, Jörg Olschewski, and Michael Ummels. Measuring permissiveness in parity games : Mean-payoff parity games revisited. *In* Tevfik Bultan and Pao-Ann Hsiung, editors, *Proceedings of the 9th International Symposium on Automated Technology for Verification and Analysis (ATVA'11), Taipei, Taiwan, October 2011*, volume 6996 of *Lecture Notes in Computer Science*, pages 135–149. Springer.

(CI-89) Thomas Brihaye, Véronique Bruyère, Laurent Doyen, Marc Ducobu, and Raskin Jean-François. Antichain-based QBF solving. *In* Tevfik Bultan and Pao-Ann Hsiung, editors, *Proceedings of the 9th International Symposium on Automated Technology for Verification and Analysis (ATVA'11), Taipei, Taiwan, October 2011*, volume 6996 of *Lecture Notes in Computer Science*, pages 183–197. Springer.

(CI-90) Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. Trace equivalence decision : Negative tests and non-determinism. *In* Yan Chen, George Danezis, and Vitaly Shmatikov, editors, *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11), Chicago, Illinois, USA, October 2011*, pages 321–330. ACM Press.

(CI-91) Laurent Fribourg, Bertrand Revol, and Romain Soulat. Synthesis of switching rules for ensuring reachability properties of sampled linear systems. *In* Yu-Fang Chen and Chao Wang, editors, *Proceedings of the 13th International Workshops on Verification of Infinite State Systems (INFINITY'11), Taipei, Taiwan, October 2011*, volume 73 of *Electronic Proceedings in Theoretical Computer Science*, pages 35–48.

(CI-92) Florent Jacquemard, Yoshiharu Kojima, and Masahiko Sakai. Controlled term rewriting. *In* Cesare Tinelli and Viorica Sofronie-Stokkermans, editors, *Proceedings of the 8th International Symposium on Frontiers of Combining Systems (FroCoS'11), Saarbrücken, Germany, October 2011*, volume 6989 of *Lecture Notes in Artificial Intelligence*, pages 179–194. Springer.

(CI-93) Fabian M. Suchanek, David Gross-Amblard, and Serge Abiteboul. Watermarking for ontologies. *In* Lora Aroyo, Chris Welty, Harith Alani, Jamie Taylor, Abraham Bernstein, Lalana Kagal, Natasha Fridman Noy, and Eva Blomqvist, editors, *Proceedings of the 10th International Semantic Web Conference (ISWC'11), Bonn, Germany, October 2011*, volume 7031 of *Lecture Notes in Computer Science*, pages 697–713. Springer.

(CI-94) Étienne André and Romain Soulat. Synthesis of timing parameters satisfying safety properties. *In* Giorgio Delzanno and Igor Potapov, editors, *Proceedings of the 5th Workshop on Reachability Problems in Computational Models (RP'11), Genova, Italy, September 2011*, volume 6945 of *Lecture Notes in Computer Science*, pages 31–44. Springer.

(CI-95) Paolo Ballarini, Hilal Djafri, Marie Duflot, Serge Haddad, and Nihal Pekergin. COSMOS : a statistical model checker for the hybrid automata stochastic logic. *In Proceedings of the 8th International Conference on Quantitative Evaluation of Systems (QEST'11), Aachen, Germany, September 2011*, pages 143–144. IEEE Computer Society Press.

(CI-96) Benedikt Bollig. An automaton over data words that captures EMSO logic. *In* Joost-Pieter Katoen and Barbara König, editors, *Proceedings of the 22nd International Conference on Concurrency Theory (CONCUR'11), Aachen, Germany, September 2011*, volume 6901 of *Lecture Notes in Computer Science*, pages 171–186. Springer.

(CI-97) Rémi Bonnet. Decidability of LTL model checking for vector addition systems with one zero-test. *In* Giorgio Delzanno and Igor Potapov, editors, *Proceedings of the 5th Workshop on Reachability Problems in Computational Models (RP'11), Genova, Italy, September 2011*, volume 6945 of *Lecture Notes in Computer Science*, pages 85–95. Springer.

(CI-98) Patricia Bouyer, Kim G. Larsen, Nicolas Markey, Ocan Sankur, and Claus Thrane. Timed automata can always be made implementable. *In* Joost-Pieter Katoen and Barbara König, editors, *Proceedings of the 22nd International Conference on Concurrency Theory (CONCUR'11), Aachen, Germany, September 2011*, volume 6901 of *Lecture Notes in Computer Science*, pages 76–91. Springer.

(CI-99) Patricia Bouyer, Nicolas Markey, and Ocan Sankur. Robust model-checking of timed automata via pumping in channel machines. *In* Uli Fahrenberg and Stavros Tripakis, editors, *Proceedings of the 9th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'11), Aalborg, Denmark, September 2011*, volume 6919 of *Lecture Notes in Computer Science*, pages 97–112. Springer.

(CI-100) Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. Bounded Parikh automata. *In* Petr Ambrož, Štěpán Holub, and Zuzana Masáková, editors, *Proceedings of the 8th International Conference WORDS (WORDS'11), Prague, Czech Republic, September 2011*, volume 63 of *Electronic Proceedings in Theoretical Computer Science*, pages 93–102.

(CI-101) Rohit Chadha, Vijay Korthikranthi, Mahesh Viswanathan, Gul Agha, and Youngmin Kwon. Model checking MDPs with a unique compact invariant set of distributions. *In Proceedings of the 8th International Conference on Quantitative Evaluation of Systems (QEST'11), Aachen, Germany, September 2011*, pages 121–130. IEEE Computer Society Press.

(CI-102) Laurent Fribourg and Ulrich Kühne. Parametric verification and test coverage for hybrid automata using the inverse method. *In* Giorgio Delzanno and Igor Potapov, editors, *Proceedings of the 5th Workshop on Reachability Problems in Computational Models (RP'11), Genova, Italy, September 2011*, volume 6945 of *Lecture Notes in Computer Science*, pages 191–204. Springer.

(CI-103) César Rodríguez, Stefan Schwoon, and Paolo Baldan. Efficient contextual unfolding. *In* Joost-Pieter Katoen and Barbara König, editors, *Proceedings of the 22nd International Conference on Concurrency Theory (CONCUR'11), Aachen, Germany, September 2011*, volume 6901 of *Lecture Notes in Computer Science*, pages 342–357. Springer.

(CI-104) Michael Ummels and Dominik Wojtczak. The complexity of Nash equilibria in limit-average games. *In* Joost-Pieter Katoen and Barbara König, editors, *Proceedings of the 22nd International Conference on Concurrency Theory (CONCUR'11), Aachen, Germany, September 2011*, volume 6901 of *Lecture Notes in Computer Science*, pages 482–496. Springer.

(CI-105) Paolo Ballarini, Hilal Djafri, Marie Duflot, Serge Haddad, and Nihal Pekergin. Petri nets compositional modeling and verification of flexible manufacturing systems. *In Proceedings of the 7th IEEE Conference on Automation Science and Engineering (CASE'11), Trieste, Italy, August 2011*, pages 588–593. IEEE Robotics & Automation Society.

(CI-106) Michel Blockelet and Sylvain Schmitz. Model-checking coverability graphs of vector addition systems. *In* Filip Murlak and Piotr Sankowski, editors, *Proceedings of the 36th International Symposium on Mathematical Foundations of Computer Science (MFCS'11), Warsaw, Poland, August 2011*, volume 6907 of *Lecture Notes in Computer Science*, pages 108–119. Springer.

(CI-107) Benedikt Bollig, Aiswarya Cyriac, Paul Gastin, and Marc Zeitoun. Temporal logics for concurrent recursive programs : Satisfiability and model checking. *In* Filip Murlak and Piotr Sankowski, editors, *Proceedings of the 36th International Symposium on Mathematical Foundations of Computer Science (MFCS'11), Warsaw, Poland, August 2011*, volume 6907 of *Lecture Notes in Computer Science*, pages 132–144. Springer.

(CI-108) Rémi Bonnet. The reachability problem for vector addition systems with one zero-test. *In* Filip Murlak and Piotr Sankowski, editors, *Proceedings of the 36th International Symposium on Mathematical Foundations of Computer Science (MFCS'11), Warsaw, Poland, August 2011*, volume 6907 of *Lecture Notes in Computer Science*, pages 145–157. Springer.

(CI-109) Krishnendu Chatterjee and Laurent Doyen. Energy and mean-payoff parity Markov decision processes. *In* Filip Murlak and Piotr Sankowski, editors, *Proceedings of the 36th International Symposium on Mathematical Foundations of Computer Science (MFCS'11), Warsaw, Poland, August 2011*, volume 6907 of *Lecture Notes in Computer Science*, pages 206–218. Springer.

(CI-110) Krishnendu Chatterjee, Laurent Doyen, and Rohit Singh. On memoryless quantitative objectives. *In* Olaf Owe, Martin Steffen, and Jan Arne Telle, editors, *Proceedings of the 18th International Symposium on Fundamentals of Computation Theory (FCT'11), Oslo, Norway, August 2011*, volume 6914 of *Lecture Notes in Computer Science*, pages 148–159. Springer.

(CI-111) Laurent Doyen, Thierry Massart, and Mahsa Shirmohammadi. Infinite synchronizing words for probabilistic automata. *In* Filip Murlak and Piotr Sankowski, editors, *Proceedings of the 36th International Symposium on Mathematical Foundations of Computer Science (MFCS'11), Warsaw, Poland, August 2011*, volume 6907 of *Lecture Notes in Computer Science*, pages 278–289. Springer.

(CI-112) Ocan Sankur. Untimed language preservation in timed systems. *In* Filip Murlak and Piotr Sankowski, editors, *Proceedings of the 36th International Symposium on Mathematical Foundations of Computer Science (MFCS'11), Warsaw, Poland, August 2011*, volume 6907 of *Lecture Notes in Computer Science*, pages 556–567. Springer.

(CI-113) Matthew Anderson, Dieter van Melkebeek, Nicole Schweikardt, and Luc Segoufin. Locality of queries definable in invariant first-order logic with arbitrary built-in predicates. *In* Luca Aceto, Monika Henzinger, and Jirí Sgall, editors, *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP'11) – Part II, Zürich, Switzerland, July 2011*, volume 6756 of *Lecture Notes in Computer Science*, pages 368–379. Springer.

(CI-114) Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Deciding security for protocols with recursive tests. *In* Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *Proceedings of the 23rd International Conference on Automated Deduction (CADE'11), Wrocław, Poland, July 2011*, Lecture Notes in Artificial Intelligence, pages 49–63. Springer.

(CI-115) Vince Bárány, Balder ten Cate, and Luc Segoufin. Guarded negation. *In* Luca Aceto, Monika Henzinger, and Jirí Sgall, editors, *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP'11) – Part II, Zürich, Switzerland, July 2011*, volume 6756 of *Lecture Notes in Computer Science*, pages 356–367. Springer.

(CI-116) Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Amélie Stainer. Emptiness and universality problems in timed automata with positive frequency. *In* Luca Aceto, Monika Henzinger, and Jirí Sgall, editors, *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP'11) – Part II, Zürich, Switzerland, July 2011*, volume 6756 of *Lecture Notes in Computer Science*, pages 246–257. Springer.

(CI-117) Thomas Brihaye, Laurent Doyen, Gilles Geeraerts, Joël Ouaknine, Jean-François Raskin, and James Worrell. On reachability for hybrid automata over bounded time. *In* Luca Aceto, Monika Henzinger, and Jirí Sgall, editors, *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP'11) – Part II, Zürich, Switzerland, July 2011*, volume 6756 of *Lecture Notes in Computer Science*, pages 416–427. Springer.

(CI-118) Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. On the expressiveness of Parikh automata and related models. *In* Rudolf Freund, Markus Holzer, Carlo Mereghetti, Friedrich Otto, and Beatrice Palano, editors, *Proceedings of the 3rd Workshop on Non-Classical Models of Automata and Applications (NCMA'11), Milano, Italy, July 2011*, volume 282 of *books@ocg.at*, pages 103–119. Austrian Computer Society.

(CI-119) Sylvain Schmitz and Philippe Schnoebelen. Multiply-recursive upper bounds with Higman's lemma. *In* Luca Aceto, Monika Henzinger, and Jirí Sgall, editors, *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP'11) – Part II, Zürich, Switzerland, July 2011*, volume 6756 of *Lecture Notes in Computer Science*, pages 441–452. Springer.

(CI-120) Serge Abiteboul, Meghyn Bienvenu, Alban Galland, and Émilien Antoine. A rule-based language for web data management. *In* Maurizio Lenzerini and Thomas Schwentick, editors, *Proceedings of the 30th Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'11), Athens, Greece, June 2011*, pages 293–304. ACM Press.

(CI-121) Serge Abiteboul, Alban Galland, and Neoklis Polyzotis. Web information management with access control. *In* Amélie Marian and Vasilis Vassalos, editors, *Proceedings of the 14th International Workshop on the Web and Databases (WebDB'11), Athens, Greece, June 2011*.

(CI-122) Sandie Balaguer, Thomas Chatain, and Stefan Haar. Building tight occurrence nets from reveals relations. *In* Benoît Caillaud and Josep Carmona, editors, *Proceedings of the 11th International Conference on Application of Concurrency to System Design (ACSD'11), Newcastle upon Tyne, UK, June 2011*, pages 44–53. IEEE Computer Society Press.

(CI-123) Pierre Chambart, Alain Finkel, and Sylvain Schmitz. Forward analysis and model checking for trace bounded WSTS. *In* Lars M. Kristensen and Laure Petrucci, editors, *Proceedings of the 32nd International Conference on Applications and Theory of Petri Nets (ICATPN'11), Newcastle upon Tyne, UK, June 2011*, volume 6709 of *Lecture Notes in Computer Science*. Springer.

(CI-124) Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel. Formal analysis of protocols based on TPM state registers. *In Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11), Cernay-la-Ville, France, June 2011*, pages 66–82. IEEE Computer Society Press.

(CI-125) Diego Figueira. A decidable two-way logic on data words. *In Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science (LICS'11), Toronto, Canada, June 2011*, pages 365–374. IEEE Computer Society Press.

(CI-126) Diego Figueira, Santiago Figueira, Sylvain Schmitz, and Philippe Schnoebelen. Ackermannian and primitive-recursive bounds with Dickson's lemma. *In Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science (LICS'11), Toronto, Canada, June 2011*, pages 269–278. IEEE Computer Society Press.

(CI-127) Jean Goubault-Larrecq and Daniele Varacca. Continuous random variables. *In Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science (LICS'11), Toronto, Canada, June 2011*, pages 97–106. IEEE Computer Society Press.

(CI-128) Stefan Haar, Christian Kern, and Stefan Schwoon. Computing the reveals relation in occurrence nets. *In* Giovanna D'Agostino and Salvatore La Torre, editors, *Proceedings of the 2nd International Symposium on Games, Automata, Logics, and Formal Verification (GandALF'11), Minori, Italy, June 2011*, volume 54 of *Electronic Proceedings in Theoretical Computer Science*, pages 31–44.

(CI-129) Serge Haddad, Jean Mairesse, and Hoang-Thach Nguyen. Synthesis and analysis of product-form Petri nets. *In* Lars M. Kristensen and Laure Petrucci, editors, *Proceedings of the 32nd International Conference on Applications and Theory of Petri Nets (ICATPN'11), Newcastle upon Tyne, UK, June 2011*, volume 6709 of *Lecture Notes in Computer Science*, pages 288–307. Springer.

(CI-130) Steve Kremer, Graham Steel, and Bogdan Warinschi. Security for key management interfaces. *In Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11), Cernay-la-Ville, France, June 2011*, pages 266–280. IEEE Computer Society Press.

(CI-131) Paolo Ballarini, Hilal Djafri, Marie Duflot, Serge Haddad, and Nihal Pekergin. HASL : An expressive language for statistical verification of stochastic models. *In Proceedings of the 5th International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS'11), Cachan, France, May 2011*, pages 306–315.

(CI-132) Émilien Antoine, Alban Galland, Kristian Lyngbaek, Amélie Marian, and Neoklis Polyzotis. Social networking on top of the webdamexchange system. *In* Serge Abiteboul, Klemens Böhm, Christoph Koch, and Kian-Lee Tan, editors, *Proceedings of the 27th International Conference on Data Engineering (ICDE'11), Hannover, Germany, April 2011*, pages 1300–1303. IEEE Computer Society Press.

(CI-133) Serge Abiteboul, Meghyn Bienvenu, Alban Galland, and Marie-Christine Rousset. Distributed Datalog revisited. *In* Oege de Moor, Georg Gottlob, Tim Furche, and Andrew Jon Sellers, editors, *Revised Selected Papers of the 1st International Workshop Datalog Reloaded (Datalog'10), Oxford, UK, March 2011*, volume 6702 of *Lecture Notes in Computer Science*, pages 252–261. Springer.

(CI-134) Serge Abiteboul, Pierre Bourhis, and Victor Vianu. Comparing workflow specification languages : a matter of views. *In* Tova Milo, editor, *Proceedings of the 14th International Conference on Database Theory (ICDT'11), Uppsala, Sweden, March 2011*, pages 78–89. ACM Press.

(CI-135) Serge Abiteboul, Balder ten Cate, and Yannis Katsis. On the equivalence of distributed systems with queries and communication. *In* Tova Milo, editor, *Proceedings of the 14th International Conference on Database Theory (ICDT'11), Uppsala, Sweden, March 2011*, pages 126–137. ACM Press.

(CI-136) Rémi Bonnet, Alain Finkel, Serge Haddad, and Fernando Rosa-Velardo. Ordinal theory for expressiveness of well structured transition systems. *In* Martin Hofmann, editor, *Proceedings of the 14th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'11), Saarbrücken, Germany, March-April 2011*, volume 6604 of *Lecture Notes in Computer Science*, pages 153–167. Springer.

(CI-137) Diego Figueira and Luc Segoufin. Bottom-up automata on data trees and vertical XPath. *In* Christoph Dürr and Thomas Schwentick, editors, *Proceedings of the 28th Annual Symposium on Theoretical Aspects of Computer Science (STACS'11), Dortmund, Germany, March 2011*, volume 9 of *Leibniz International Proceedings in Informatics*, pages 93–104. Leibniz-Zentrum für Informatik.

(CI-138) Daniel Pasailă. Conjunctive queries determinacy and rewriting. *In* Tova Milo, editor, *Proceedings of the 14th International Conference on Database Theory (ICDT'11), Uppsala, Sweden, March 2011*, pages 220–231. ACM Press.

(CI-139) Luc Segoufin and Szymon Toruńczyk. Automata based verification over linearly ordered data domains. *In* Christoph Dürr and Thomas Schwentick, editors, *Proceedings of the 28th Annual Symposium on Theoretical Aspects of Computer Science (STACS'11), Dortmund, Germany, March 2011*, volume 9 of *Leibniz International Proceedings in Informatics*, pages 81–92. Leibniz-Zentrum für Informatik.

(CI-140) Balder ten Cate and Luc Segoufin. Unary negation. *In* Christoph Dürr and Thomas Schwentick, editors, *Proceedings of the 28th Annual Symposium on Theoretical Aspects of Computer Science (STACS'11), Dortmund, Germany, March 2011*, volume 9 of *Leibniz International Proceedings in Informatics*, pages 344–355. Leibniz-Zentrum für Informatik.

(CI-141) Michel Abdalla, Céline Chevalier, Louis Granboulan, and David Pointcheval. Contributory password-authenticated group key exchange with join capability. *In* Aggelos Kiayias, editor, *Proceedings of the Cryptographers' Track at the RSA Conference 2011 (CT-RSA'11), San Francisco, California, USA, February 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 142–160. Springer.

(CI-142) Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. Probabilistic büchi automata with non-extremal acceptance thresholds. *In* Ranjit Jhala and David Schmidt, editors, *Proceedings of the 12th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'11), Austin, Texas, USA, January 2011*, volume 6538 of *Lecture Notes in Computer Science*, pages 103–117. Springer.

(CI-143) S. Akshay, Paul Gastin, Madhavan Mukund, and K. Narayan Kumar. Model checking time-constrained scenario-based specifications. *In* Kamal Lodaya and Meena Mahajan, editors, *Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10), Chennai, India, December 2010*, volume 8 of *Leibniz International Proceedings in Informatics*, pages 204–215. Leibniz-Zentrum für Informatik.

(CI-144) Rémi Bonnet, Alain Finkel, Jérôme Leroux, and Marc Zeitoun. Place-boundedness for vector addition systems with one zero-test. *In* Kamal Lodaya and Meena Mahajan, editors, *Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10), Chennai, India, December 2010*, volume 8 of *Leibniz International Proceedings in Informatics*, pages 192–203. Leibniz-Zentrum für Informatik.

(CI-145) Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. Model checking concurrent programs with nondeterminism and randomization. *In* Kamal Lodaya and Meena Mahajan, editors, *Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10), Chennai, India, December 2010*, volume 8 of *Leibniz International Proceedings in Informatics*, pages 364–375. Leibniz-Zentrum für Informatik.

(CI-146) Krishnendu Chatterjee, Laurent Doyen, Thomas A. Henzinger, and Jean-François Raskin. Generalized mean-payoff and energy games. *In* Kamal Lodaya and Meena Mahajan, editors, *Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10), Chennai, India, December 2010*, volume 8 of *Leibniz International Proceedings in Informatics*, pages 505–516. Leibniz-Zentrum für Informatik.

(CI-147) Arnaud Da Costa, François Laroussinie, and Nicolas Markey. ATL with strategy contexts : Expressiveness and model checking. *In* Kamal Lodaya and Meena Mahajan, editors, *Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10), Chennai, India, December 2010*, volume 8 of *Leibniz International Proceedings in Informatics*, pages 120–132. Leibniz-Zentrum für Informatik.

(CI-148) Paul Hunter, Patricia Bouyer, Nicolas Markey, Joël Ouaknine, and James Worrell. Computing rational radical sums in uniform TC^0. *In* Kamal Lodaya and Meena Mahajan, editors, *Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'10), Chennai, India, December 2010*, volume 8 of *Leibniz International Proceedings in Informatics*, pages 308–316. Leibniz-Zentrum für Informatik.

(CI-149) Ryma Abassi, Florent Jacquemard, Michaël Rusinowitch, and Sihem Guemara El Fatmi. XML access control : from XACML to annotated schemas. *In Proceedings of the 2nd International Conference on Communications and Networking (ComNet'10), Tozeur, Tunisia, November 2010*. IEEE Computer Society Press.

(CI-150) Sebastian S. Bauer, Rolf Hennicker, and Michel Bidoit. A modal interface theory with data constraints. *In* Jim Davies, Leila Silva, and Adenilso da Silva Simão, editors, *Revised Selected Papers of the 13th Brazilian Symposium on Formal Methods (SBMF'10), , November 2010*, volume 6527 of *Lecture Notes in Computer Science*, pages 80–95. Springer.

(CI-151) Matteo Bortolozzo, Matteo Centenaro, Riccardo Focardi, and Graham Steel. Attacking and fixing PKCS#11 security tokens. *In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10), Chicago, Illinois, USA, October 2010*, pages 260–269. ACM Press.

(CI-152) Ulrich Kühne, Sven Beyer, Jörg Bormann, and John Barstow. Automated formal verification of processors based on architectural models. *In* Roderick Bloem and Natasha Sharygina, editors, *Proceedings of the 10th International Conference on Formal Methods in Computer Aided Design (FMCAD'10), Lugano, Switzerland, October 2010*, pages 129–136. IEEE Computer Society Press.

(CI-153) Ben Smyth, Mark D. Ryan, Steve Kremer, and Mounira Kourjieh. Towards automatic analysis of election verifiability properties. *In* Alessandro Armando and Gavin Lowe, editors, *Proceedings of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'10), Paphos, Cyprus, March 2010*, volume 6186 of *Lecture Notes in Computer Science*, pages 146–163. Springer, October 2010.

(CI-154) Serge Abiteboul, Pierre Bourhis, Bogdan Marinoiu, and Alban Galland. AXART – Enabling collaborative work with AXML artifacts. *In* Yi Chen and Y.C. Tay, editors, *Proceedings of the 36th International Conference on Very Large Data Bases (VLDB'10), Singapore, September 2010*, volume 3 of *Proceedings of the VLDB Endowment*, pages 1553–1556. ACM Press.

(CI-155) Étienne André. IMITATOR II : A tool for solving the good parameters problem in timed automata. *In* Yu-Fang Chen and Ahmed Rezine, editors, *Proceedings of the 12th International Workshops on Verification of Infinite State Systems (INFINITY'10), Singapore, September 2010*, volume 39 of *Electronic Proceedings in Theoretical Computer Science*, pages 91–99.

(CI-156) Sandie Balaguer, Thomas Chatain, and Stefan Haar. A concurrency-preserving translation from time Petri nets to networks of timed automata. *In* Nicolas Markey and Jef Wijsen, editors, *Proceedings of the 17th International Symposium on Temporal Representation and Reasoning (TIME'10), Paris, France, September 2010*, pages 77–84. IEEE Computer Society Press.

(CI-157) Paolo Baldan, Alessandro Bruni, Andrea Corradini, Barbara König, and Stefan Schwoon. On the computation of McMillan's prefix for contextual nets and graph grammars. *In* Hartmut Ehrig, Arend Rensink, Grzegorz Rozenberg, and Andy Schürr, editors, *Proceedings of the 5th International Conference on Graph Transformations (ICGT'10), Enschede, The Netherlands, September-October 2010*, volume 6372 of *Lecture Notes in Computer Science*, pages 91–106. Springer.

(CI-158) Béatrice Bérard, Serge Haddad, and Mathieu Sassolas. Real time properties for interrupt timed automata. *In* Nicolas Markey and Jef Wijsen, editors, *Proceedings of the 17th International Symposium on Temporal Representation and Reasoning (TIME'10), Paris, France, September 2010*, pages 69–76. IEEE Computer Society Press.

(CI-159) Patricia Bouyer, Romain Brenguier, and Nicolas Markey. Computing equilibria in two-player timed games *via* turn-based finite games. *In* Krishnendu Chatterjee and Thomas A. Henziner, editors, *Proceedings of the 8th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'10), Vienna, Austria, September 2010*, volume 6246 of *Lecture Notes in Computer Science*, pages 62–76. Springer.

(CI-160) Morten Dahl, Stéphanie Delaune, and Graham Steel. Formal analysis of privacy for vehicular mix-zones. *In* Dimitris Gritzalis and Bart Preneel, editors, *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10), Athens, Greece, September 2010*, volume 6345 of *Lecture Notes in Computer Science*, pages 55–70. Springer.

(CI-161) Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel. A formal analysis of authentication in the TPM. *In* Pierpaolo Degano, Sandro Etalle, and Joshua Guttman, editors, *Revised Selected Papers of the 7th International Workshop on Formal Aspects in Security and Trust (FAST'10), Pisa, Italy, September 2010*, volume 6561 of *Lecture Notes in Computer Science*, pages 111–125. Springer.

(CI-162) Stéphane Demri. On selective unboundedness of VASS. *In* Yu-Fang Chen and Ahmed Rezine, editors, *Proceedings of the 12th International Workshops on Verification of Infinite State Systems (INFINITY'10), Singapore, September 2010*, volume 39 of *Electronic Proceedings in Theoretical Computer Science*, pages 1–15.

(CI-163) Serge Haddad, Lynda Mokdad, and Samir Youcef. Selection of the best composite web service based on quality of service. *In* Witold Abramowicz, Rainer Alt, Klaus-Peter Fähnrich, Bogdan Franczyk, and Leszek A. Maciaszek, editors, *Proceedings of the 2nd International Symposium on Services Science and 3rd International Conference on Business Process and Services Computing (ISSS/BPSC'10), Leipzig, Germany, September-October 2010*, volume 177 of *Lecture Notes in Informatics*, pages 255–266. Gesellschaft für Informatik.

(CI-164) Steve Kremer, Mark D. Ryan, and Ben Smyth. Election verifiability in electronic voting protocols. *In* Dimitris Gritzalis and Bart Preneel, editors, *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10), Athens, Greece, September 2010*, volume 6345 of *Lecture Notes in Computer Science*, pages 389–404. Springer.

(CI-165) Étienne André and Laurent Fribourg. Behavioral cartography of timed automata. *In* Antonín Kučera and Igor Potapov, editors, *Proceedings of the 4th Workshop on Reachability Problems in*

Computational Models (RP'10), Brno, Czech Republic, August 2010, volume 6227 of *Lecture Notes in Computer Science*, pages 76–90. Springer.

(CI-166) Patricia Bouyer, Romain Brenguier, and Nicolas Markey. Nash equilibria for reachability objectives in multi-player timed games. *In* Paul Gastin and François Laroussinie, editors, *Proceedings of the 21st International Conference on Concurrency Theory (CONCUR'10), Paris, France, August-September 2010*, volume 6269 of *Lecture Notes in Computer Science*, pages 192–206. Springer.

(CI-167) Pierre Chambart and Philippe Schnoebelen. Computing blocker sets for the regular Post embedding problem. *In* Yuan Gao, Hanlin Lu, Shinnosuke Seki, and Sheng Yu, editors, *Proceedings of the 14th International Conference on Developments in Language Theory (DLT'10), London, Ontario, Canada, August 2010*, volume 6224 of *Lecture Notes in Computer Science*, pages 136–147. Springer.

(CI-168) Krishnendu Chatterjee, Laurent Doyen, Herbert Edelsbrunner, Thomas A. Henzinger, and Philippe Rannou. Mean-payoff automaton expressions. *In* Paul Gastin and François Laroussinie, editors, *Proceedings of the 21st International Conference on Concurrency Theory (CONCUR'10), Paris, France, August-September 2010*, volume 6269 of *Lecture Notes in Computer Science*, pages 269–283. Springer.

(CI-169) Krishnendu Chatterjee, Laurent Doyen, Hugo Gimbert, and Thomas A. Henzinger. Randomness for free. *In* Petr Hliněný and Antonín Kučera, editors, *Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS'10), Brno, Czech Republic, August 2010*, volume 6281 of *Lecture Notes in Computer Science*, pages 246–257. Springer.

(CI-170) Krishnendu Chatterjee, Laurent Doyen, and Thomas A. Henzinger. Qualitative analysis of partially-observable Markov decision processes. *In* Petr Hliněný and Antonín Kučera, editors, *Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS'10), Brno, Czech Republic, August 2010*, volume 6281 of *Lecture Notes in Computer Science*, pages 258–269. Springer.

(CI-171) Aldric Degorre, Laurent Doyen, Raffaella Gentilini, Jean-François Raskin, and Szymon Toruńczyk. Energy and mean-payoff games with imperfect information. *In* Anuj Dawar and Helmut Veith, editors, *Proceedings of the 19th Annual EACSL Conference on Computer Science Logic (CSL'10), Brno, Czech Republic, August 2010*, volume 6247 of *Lecture Notes in Computer Science*, pages 260–274. Springer.

(CI-172) Diego Figueira, Piotr Hofman, and Sławomir Lasota. Relating timed and register automata. *In* Sibylle Fröschle and Franck Valencia, editors, *Proceedings of the 17th International Workshop on Expressiveness in Concurrency (EXPRESS'10), Paris, France, August 2010*, volume 41 of *Electronic Proceedings in Theoretical Computer Science*, pages 61–75.

(CI-173) Gaëlle Fontaine and Thomas Place. Classes of trees definable in the μ-calculus. *In* Petr Hliněný and Antonín Kučera, editors, *Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS'10), Brno, Czech Republic, August 2010*, volume 6281 of *Lecture Notes in Computer Science*, pages 381–392. Springer.

(CI-174) Stefan Haar. What topology tells us about diagnosability in partial order semantics. *In Proceedings of the 10th Workshop on Discrete Event Systems (WODES'10), Berlin, Germany, August-September 2010*, pages 221–226.

(CI-175) Jörg Olschewski and Michael Ummels. The complexity of finding reset words in finite automata. *In* Petr Hliněný and Antonín Kučera, editors, *Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS'10), Brno, Czech Republic, August 2010*, volume 6281 of *Lecture Notes in Computer Science*, pages 568–579. Springer.

(CI-176) Philippe Schnoebelen. Revisiting Ackermann-hardness for lossy counter machines and reset Petri nets. *In* Petr Hliněný and Antonín Kučera, editors, *Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS'10), Brno, Czech Republic, August 2010*, volume 6281 of *Lecture Notes in Computer Science*, pages 616–628. Springer.

(CI-177) Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Modeling and verifying ad hoc routing protocols. *In Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10), Edinburgh, Scotland, UK, July 2010*, pages 59–74. IEEE Computer Society Press.

(CI-178) Luis Barguñó, Carles Creus, Guillem Godoy, Florent Jacquemard, and Camille Vacher. The emptiness problem for tree automata with global constraints. *In Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science (LICS'10), Edinburgh, Scotland, UK, July 2010*, pages 263–272. IEEE Computer Society Press.

(CI-179) Benedikt Bollig, Paul Gastin, Benjamin Monmege, and Marc Zeitoun. Pebble weighted automata and transitive closure logics. *In* Samson Abramsky, Friedhelm Meyer auf der Heide, and Paul Spirakis, editors, *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP'10) – Part II, Bordeaux, France, July 2010*, volume 6199 of *Lecture Notes in Computer Science*, pages 587–598. Springer.

(CI-180) Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, Martin Leucker, Daniel Neider, and David R. Piegdon. libalf : the automata learning framework. *In* Byron Cook, Paul Jackson, and Tayssir Touili, editors, *Proceedings of the 22nd International Conference on Computer Aided Verification (CAV'10), Edinburgh, Scotland, UK, July 2010*, volume 6174 of *Lecture Notes in Computer Science*, pages 360–364. Springer.

(CI-181) Pierre Chambart and Philippe Schnoebelen. Pumping and counting on the regular Post embedding problem. *In* Samson Abramsky, Friedhelm Meyer auf der Heide, and Paul Spirakis, editors, *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP'10) – Part II, Bordeaux, France, July 2010*, volume 6199 of *Lecture Notes in Computer Science*, pages 64–75. Springer.

(CI-182) Krishnendu Chatterjee and Laurent Doyen. Energy parity games. *In* Samson Abramsky, Friedhelm Meyer auf der Heide, and Paul Spirakis, editors, *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP'10) – Part II, Bordeaux, France, July 2010*, volume 6199 of *Lecture Notes in Computer Science*, pages 599–610. Springer.

(CI-183) Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. Automating security analysis : symbolic equivalence of constraint systems. *In* Jürgen Giesl and Reiner Haehnle, editors, *Proceedings of the 5th International Joint Conference on Automated Reasoning (IJCAR'10), Edinburgh, Scotland, UK, July 2010*, volume 6173 of *Lecture Notes in Artificial Intelligence*, pages 412–426. Springer-Verlag.

(CI-184) Ştefan Ciobâcă and Véronique Cortier. Protocol composition for arbitrary primitives. *In Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10), Edinburgh, Scotland, UK, July 2010*, pages 322–336. IEEE Computer Society Press.

(CI-185) Jean Goubault-Larrecq. ω**QRB**-domains and the probabilistic powerdomain. *In Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science (LICS'10), Edinburgh, Scotland, UK, July 2010*, pages 352–361. IEEE Computer Society Press.

(CI-186) Florent Jacquemard and Michaël Rusinowitch. Rewrite-based verification of XML updates. *In* Temur Kutsia, Wolfgang Schreiner, and Maribel Fernández, editors, *Proceedings of the 12th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming (PPDP'10), Hagenberg, Austria, July 2010*, pages 119–130. ACM Press.

(CI-187) Thomas Place and Luc Segoufin. Deciding definability in $FO_2(<)$ on trees. *In Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science (LICS'10), Edinburgh, Scotland, UK, July 2010*, pages 253–262. IEEE Computer Society Press.

(CI-188) Sylvain Schmitz. On the computational complexity of dominance links in grammatical formalisms. *In Proceedings of the 48th Annual Meeting of the Association for Computational Linguistics (ACL'10), Uppsala, Sweden, July 2010*, pages 514–524. Association for Computational Linguistics.

(CI-189) Nicole Schweikardt and Luc Segoufin. Addition-invariant FO and regularity. *In Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science (LICS'10), Edinburgh, Scotland, UK, July 2010*, pages 273–282. IEEE Computer Society Press.

(CI-190) Benedikt Bollig and Loïc Hélouët. Realizability of dynamic MSC languages. *In* Ernst W. Mayr, editor, *Proceedings of the 5th International Computer Science Symposium in Russia (CSR'10), Kazan, Russia, June 2010*, volume 6072 of *Lecture Notes in Computer Science*, pages 48–59. Springer.

(CI-191) Thomas Chatain and Éric Fabre. Factorization properties of symbolic unfoldings of colored Petri nets. *In* Johan Lilius and Wojciech Penczek, editors, *Proceedings of the 31st International Conference on Applications and Theory of Petri Nets (ICATPN'10), Braga, Portugal, June 2010*, volume 6128 of *Lecture Notes in Computer Science*, pages 165–184. Springer.

(CI-192) Serge Haddad, Lynda Mokdad, and Samir Youcef. Response time of BPEL4WS constructors. *In Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC'10), Riccione, Italy, June 2010*, pages 695–700. IEEE Computer Society Press.

(CI-193) Mehdi Ben Hmida and Serge Haddad. Client synthesis for aspect oriented web services. *In* Christine Choppy and Oleg Sokolsky, editors, *Revised Selected Papers of the 15th Monterey Workshop on Foundations of Computer Software (MONTEREY'08), Budapest, Hungary, September 2008*, volume 6028 of *Lecture Notes in Computer Science*, pages 24–42. Springer, April 2010.

(CI-194) Patricia Bouyer, Uli Fahrenberg, Kim G. Larsen, and Nicolas Markey. Timed automata with observers under energy constraints. *In* Karl Henrik Johansson and Wang Yi, editors, *Proceedings of the 13th International Conference on Hybrid Systems : Computation and Control (HSCC'10), Stockholm, Sweden, April 2010*, pages 61–70. ACM Press.

(CI-195) Serge Abiteboul, T.-H. Hubert Chan, Evgeny Kharlamov, Werner Nutt, and Pierre Senellart. Aggregate queries for discrete and continuous probabilistic XML. *In* Luc Segoufin, editor, *Proceedings of the 13th International Conference on Database Theory (ICDT'10), Lausanne, Switzerland, March 2010*, pages 50–61. ACM Press.

(CI-196) Pierre Chambart and Philippe Schnoebelen. Toward a compositional theory of leftist grammars and transformations. *In* C.-H. Luke Ong, editor, *Proceedings of the 13th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'10), Paphos, Cyprus, March 2010*, volume 6014 of *Lecture Notes in Computer Science*, pages 237–251. Springer.

(CI-197) Stéphane Demri and Arnaud Sangnier. When model-checking freeze LTL over counter machines becomes decidable. *In* C.-H. Luke Ong, editor, *Proceedings of the 13th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'10), Paphos, Cyprus, March 2010*, volume 6014 of *Lecture Notes in Computer Science*, pages 176–190. Springer.

(CI-198) Diego Figueira. Forward-XPath and extended register automata on data-trees. *In* Luc Segoufin, editor, *Proceedings of the 13th International Conference on Database Theory (ICDT'10), Lausanne, Switzerland, March 2010*, pages 230–240. ACM Press.

(CI-199) Balder ten Cate and Gaëlle Fontaine. An easy completeness proof for the modal μ-calculus on finite trees. *In* C.-H. Luke Ong, editor, *Proceedings of the 13th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'10), Paphos, Cyprus, March 2010*, volume 6014 of *Lecture Notes in Computer Science*, pages 161–175. Springer.

(CI-200) Jules Villard, Étienne Lozes, and Cristiano Calcagno. Tracking heaps that hop with heap-hop. *In* Javier Esparza and Rupak Majumdar, editors, *Proceedings of the 16th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'10), Paphos, Cyprus, March 2010*, volume 6015 of *Lecture Notes in Computer Science*, pages 275–279. Springer.

(CI-201) Alban Galland, Serge Abiteboul, Amélie Marian, and Pierre Senellart. Corroborating information from disagreeing views. *In* Brian D. Davison, Torsten Suel, Nick Craswell, and Bing Liu, editors, *Proceedings of the 3rd International Conference on Web Search and Web Data Mining (WSDM'10), New York, New York, USA, February 2010*, pages 131–140. ACM Press.

(CI-202) Rohit Chadha, Axel Legay, Pavithra Prabhakar, and Mahesh Viswanathan. Complexity bounds for the verification of real-time software. *In* Gilles Barthe and Manuel Hermenegildo, editors, *Proceedings of the 11th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'10), Madrid, Spain, January 2010*, volume 5944 of *Lecture Notes in Computer Science*, pages 95–111. Springer.

(CI-203) Alain Finkel and Arnaud Sangnier. Mixing coverability and reachability to analyze VASS with one zero-test. *In* David Peleg and Anca Muscholl, editors, *Proceedings of the 36th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'10), Špindlerův Mlýn, Czech Republic, January 2010*, volume 5901 of *Lecture Notes in Computer Science*, pages 394–406. Springer.

(CI-204) Sergiu Bursuc, Stéphanie Delaune, and Hubert Comon-Lundh. Deducibility constraints. *In* Anupam Datta, editor, *Proceedings of the 13th Asian Computing Science Conference (ASIAN'09), Seoul, Korea, December 2009*, volume 5913 of *Lecture Notes in Computer Science*, pages 24–38. Springer.

(CI-205) Stéphanie Delaune, Steve Kremer, and Olivier Pereira. Simulation based security in the applied pi calculus. *In* Ravi Kannan and K. Narayan Kumar, editors, *Proceedings of the 29th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'09), Kanpur, India, December 2009*, volume 4 of *Leibniz International Proceedings in Informatics*, pages 169–180. Leibniz-Zentrum für Informatik.

(CI-206) Stéphane Demri, Marcin Jurdziński, Oded Lachish, and Ranko Lazić. The covering and boundedness problems for branching vector addition systems. *In* Ravi Kannan and K. Narayan Kumar, editors, *Proceedings of the 29th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'09), Kanpur, India, December 2009*, volume 4 of *Leibniz International Proceedings in Informatics*, pages 181–192. Leibniz-Zentrum für Informatik.

(CI-207) Stefan Haar. Qualitative diagnosability of labeled Petri nets revisited. *In Proceedings of the Joint 48th IEEE Conference on Decision and Control (CDC'09) and 28th Chinese Control Conference (CCC'09), Shanghai, China, December 2009*, pages 1248–1253. IEEE Control System Society.

(CI-208) Steve Kremer, Antoine Mercier, and Ralf Treinen. Reducing equational theories for the decision of static equivalence. *In* Anupam Datta, editor, *Proceedings of the 13th Asian Computing Science Conference (ASIAN'09), Seoul, Korea, December 2009*, volume 5913 of *Lecture Notes in Computer Science*, pages 94–108. Springer.

(CI-209) Jules Villard, Étienne Lozes, and Cristiano Calcagno. Proving copyless message passing. *In* Zhenjiang Hu, editor, *Proceedings of the 7th Asian Symposium on Programming Languages and Systems (APLAS'09), Seoul, Korea, December 2009*, volume 5904 of *Lecture Notes in Computer Science*, pages 194–209. Springer.

(CI-210) Étienne André and Laurent Fribourg. An inverse method for policy-iteration based algorithms. *In* Azadeh Farzan and Axel Legay, editors, *Proceedings of the 11th International Workshops on Verification of Infinite State Systems (INFINITY'09), Bologna, Italy, August 2009*, volume 10 of *Electronic Proceedings in Theoretical Computer Science*, pages 44–61.

(CI-211) Florent Bouchy, Alain Finkel, and Pierluigi San Pietro. Dense-choice counter machines revisited. *In* Azadeh Farzan and Axel Legay, editors, *Proceedings of the 11th International Workshops on Verification of Infinite State Systems (INFINITY'09), Bologna, Italy, August 2009*, volume 10 of *Electronic Proceedings in Theoretical Computer Science*, pages 3–22.

(CI-212) Frédéric Dadeau, Pierre-Cyrille Héam, and Jocelyn Levrey. On the use of uniform random generation of automata for testing. *In Proceedings of the 5th Workshop on Model-Based Testing (MBT'09), York, UK, March 2009*, volume 253(2) of *Electronic Notes in Theoretical Computer Science*, pages 37–51. Elsevier Science Publishers, October 2009.

(CI-213) Alain Finkel, Étienne Lozes, and Arnaud Sangnier. Towards model checking pointer systems. *In* Margaret Archibald, Vasco Brattka, Valentin Goranko, and Benedikt Löwe, editors, *Revised Selected Papers of the International Conference on Infinity in Logic & Computation (ILC'07), Cape Town, South Africa, November 2007*, volume 5489 of *Lecture Notes in Artificial Intelligence*, pages 56–82. Springer-Verlag, October 2009.

(CI-214) Riccardo Focardi, Flaminia L. Luccio, and Graham Steel. Blunting differential attacks on PIN processing APIs. *In* Audun Jøsang, Torleiv Maseng, and Svein Johan Knapskog, editors, *Proceedings of the 14th Nordic Workshop on Secure IT Systems (NordSec'09), Oslo, Norway, October 2009*, volume 5838 of *Lecture Notes in Computer Science*, pages 88–103. Springer.

(CI-215) Étienne André, Laurent Fribourg, and Jeremy Sproston. An extension of the inverse method to probabilistic timed automata. *In* Markus Roggenbach, editor, *Proceedings of the 9th International Workshop on Automated Verification of Critical Systems (AVoCS'09), Swansea, UK, September 2009*, volume 23 of *Electronic Communications of the EASST*. European Association of Software Science and Technology.

(CI-216) Yohan Boichut, Pierre-Cyrille Héam, and Olga Kouchnarenko. How to tackle integer weighted automata positivity. *In* Olivier Bournez and Igor Potapov, editors, *Proceedings of the 3rd Workshop on Reachability Problems in Computational Models (RP'09), Palaiseau, France, September 2009*, volume 5797 of *Lecture Notes in Computer Science*, pages 79–92. Springer.

(CI-217) Anne Bouillard, Stefan Haar, and Sidney Rosario. Critical paths in the partial order unfolding of a stochastic Petri net. *In* Joël Ouaknine and Frits Vaandrager, editors, *Proceedings of the 7th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'09), Budapest, Hungary, September 2009*, volume 5813 of *Lecture Notes in Computer Science*, pages 43–57. Springer.

(CI-218) Patricia Bouyer, Marie Duflot, Nicolas Markey, and Gabriel Renault. Measuring permissivity in finite games. *In* Mario Bravetti and Gianluigi Zavattaro, editors, *Proceedings of the 20th International Conference on Concurrency Theory (CONCUR'09), Bologna, Italy, September 2009*, volume 5710 of *Lecture Notes in Computer Science*, pages 196–210. Springer.

(CI-219) Peter Bulychev, Thomas Chatain, Alexandre David, and Kim G. Larsen. Checking simulation relation between timed game automata. *In* Joël Ouaknine and Frits Vaandrager, editors, *Proceedings of the 7th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'09), Budapest, Hungary, September 2009*, volume 5813 of *Lecture Notes in Computer Science*, pages 73–87. Springer.

(CI-220) Matteo Centenaro, Riccardo Focardi, Flaminia L. Luccio, and Graham Steel. Type-based analysis of PIN processing APIs. *In* Michael Backes and Peng Ning, editors, *Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS'09), Saint Malo, France, September 2009*, volume 5789 of *Lecture Notes in Computer Science*, pages 53–68. Springer.

(CI-221) Véronique Cortier and Graham Steel. A generic security API for symmetric key management on cryptographic devices. *In* Michael Backes and Peng Ning, editors, *Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS'09), Saint Malo, France, September 2009*, volume 5789 of *Lecture Notes in Computer Science*, pages 605–620. Springer.

(CI-222) Serge Haddad and Nihal Pekergin. Using stochastic comparison for efficient model checking of uncertain Markov chains. *In Proceedings of the 6th International Conference on Quantitative Evaluation of Systems (QEST'09), Budapest, Hungary, September 2009*, pages 177–186. IEEE Computer Society Press.

(CI-223) Étienne André. IMITATOR : A tool for synthesizing constraints on timing bounds of timed automata. *In* Martin Leucker and Carroll Morgan, editors, *Proceedings of the 6th International Colloquium on Theoretical Aspects of Computing (ICTAC'09), Kuala Lumpur, Malaysia, August 2009*, volume 5684 of *Lecture Notes in Computer Science*, pages 336–342. Springer.

(CI-224) Ştefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. Computing knowledge in security protocols under convergent equational theories. *In* Renate Schmidt, editor, *Proceedings of the 22nd International Conference on Automated Deduction (CADE'09), Montreal, Canada, August 2009*, Lecture Notes in Artificial Intelligence, pages 355–370. Springer.

(CI-225) Diego Figueira and Luc Segoufin. Future-looking logics on data words and trees. *In* Rastislav Královič and Damian Niwiński, editors, *Proceedings of the 34th International Symposium on Mathematical Foundations of Computer Science (MFCS'09), Novy Smokovec, Slovakia, August 2009*, volume 5734 of *Lecture Notes in Computer Science*, pages 331–343. Springer.

(CI-226) Sibylle Fröschle and Graham Steel. Analysing PKCS#11 key management APIs with unbounded fresh data. *In* Pierpaolo Degano and Luca Viganò, editors, *Revised Selected Papers of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09), York, UK, March 2009*, volume 5511 of *Lecture Notes in Computer Science*, pages 92–106. Springer, August 2009.

(CI-227) Gavin Keighren, David Aspinall, and Graham Steel. Towards a type system for security APIs. *In* Pierpaolo Degano and Luca Viganò, editors, *Revised Selected Papers of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09), York, UK, March 2009*, volume 5511 of *Lecture Notes in Computer Science*, pages 173–192. Springer, August 2009.

(CI-228) Delphine Longuet and Marc Aiguier. Integration testing from structured first-order specifications via deduction modulo. *In* Martin Leucker and Carroll Morgan, editors, *Proceedings of the 6th International Colloquium on Theoretical Aspects of Computing (ICTAC'09), Kuala Lumpur, Malaysia, August 2009*, volume 5684 of *Lecture Notes in Computer Science*, pages 261–276. Springer.

(CI-229) Carlos Areces and Diego Figueira. Which semantics for neighbourhood semantics ? *In* Craig Boutilier, editor, *Proceedings of the 21st International Joint Conference on Artificial Intelligence (IJCAI'09), Pasadena, California, USA, July 2009*, pages 671–676. AAAI Press.

(CI-230) Carlos Areces, Diego Figueira, Daniel Gorín, and Sergio Mera. Tableaux and model checking for memory logics. *In* Martin Giese and Arild Waaler, editors, *Proceedings of the 18th International Workshop on Theorem Proving with Analytic Tableaux and Related Methods (TABLEAUX'09), Oslo, Norway, July 2009*, volume 5607 of *Lecture Notes in Artificial Intelligence*, pages 47–61. Springer.

(CI-231) Christel Baier, Nathalie Bertrand, Patricia Bouyer, and Thomas Brihaye. When are timed automata determinizable ? *In* Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, and Wolfgang Thomas, editors, *Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP'09), Rhodes, Greece, July 2009*, volume 5556 of *Lecture Notes in Computer Science*, pages 43–54. Springer.

(CI-232) Nihel Ben Youssef, Adel Bouhoula, and Florent Jacquemard. Automatic verification of conformance of firewall configurations to security policies. *In Proceedings of the 14th IEEE Symposium on Computers and Communications (ISCC'09), Sousse, Tunisia, July 2009*, pages 526 – 531. IEEE Computer Society Press.

(CI-233) Benedikt Bollig, Peter Habermehl, Carsten Kern, and Martin Leucker. Angluin-style learning of NFA. *In* Craig Boutilier, editor, *Proceedings of the 21st International Joint Conference on Artificial Intelligence (IJCAI'09), Pasadena, California, USA, July 2009*, pages 1004–1009. AAAI Press.

(CI-234) Florent Bouchy, Alain Finkel, and Arnaud Sangnier. Reachability in timed counter systems. *In* Peter Habermehl and Tomáš Vojnar, editors, *Joint Proceedings of the 8th, 9th and 10th International Workshops on Verification of Infinite State Systems (INFINITY'06,'07,'08)*, volume 239 of *Electronic Notes in Theoretical Computer Science*, pages 167–178. Elsevier Science Publishers, July 2009.

(CI-235) Patricia Bouyer and Vojtěch Forejt. Reachability in stochastic timed games. *In* Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, and Wolfgang Thomas, editors, *Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP'09), Rhodes, Greece, July 2009*, volume 5556 of *Lecture Notes in Computer Science*, pages 103–114. Springer.

(CI-236) Véronique Cortier and Stéphanie Delaune. A method for proving observational equivalence. *In Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09), Port Jefferson, New York, USA, July 2009*, pages 266–276. IEEE Computer Society Press.

(CI-237) Roméo Courbis, Pierre-Cyrille Héam, and Olga Kouchnarenko. TAGED approximations for veriying temporal patterns. *In* Sebastian Maneth, editor, *Proceedings of the 14th International Conference on Implementation and Application of Automata (CIAA'09), Sydney, Australia, July 2009*, volume 5642 of *Lecture Notes in Computer Science*, pages 135–144. Springer-Verlag.

(CI-238) Emmanuelle Encrenaz and Alain Finkel. Automatic verification of counter systems with ranking functions. *In* Peter Habermehl and Tomáš Vojnar, editors, *Joint Proceedings of the 8th, 9th and 10th International Workshops on Verification of Infinite State Systems (INFINITY'06,'07,'08)*, volume 239 of *Electronic Notes in Theoretical Computer Science*, pages 85–103. Elsevier Science Publishers, July 2009.

(CI-239) Alain Finkel and Jean Goubault-Larrecq. Forward analysis for WSTS, part II : Complete WSTS. *In* Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, and Wolfgang Thomas, editors, *Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP'09), Rhodes, Greece, July 2009*, volume 5556 of *Lecture Notes in Computer Science*, pages 188–199. Springer.

(CI-240) Pierre-Cyrille Héam, Cyril Nicaud, and Sylvain Schmitz. Random generation of deterministic tree (walking) automata. *In* Sebastian Maneth, editor, *Proceedings of the 14th International Conference on Implementation and Application of Automata (CIAA'09), Sydney, Australia, July 2009*, volume 5642 of *Lecture Notes in Computer Science*, pages 115–124. Springer-Verlag.

(CI-241) Thomas Place and Luc Segoufin. A decidable characterization of locally testable tree languages. *In* Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, and Wolfgang Thomas, editors, *Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP'09), Rhodes, Greece, July 2009*, volume 5556 of *Lecture Notes in Computer Science*, pages 285–296. Springer.

(CI-242) Serge Abiteboul, Pierre Bourhis, and Bogdan Marinoiu. Satisfiability and relevance for queries over active documents. *In* Jianwen Su, editor, *Proceedings of the 28th Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'09), Providence, Rhode Island, USA, June-July 2009*, pages 87–96. ACM Press.

(CI-243) Serge Abiteboul, Georg Gottlob, and Marco Manna. Distributed XML design. *In* Jianwen Su, editor, *Proceedings of the 28th Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'09), Providence, Rhode Island, USA, June-July 2009*, pages 247–258. ACM Press.

(CI-244) Pablo Barceló, Leonid Libkin, Antonella Poggi, and Cristina Sirangelo. XML with incomplete information : Models, properties, and query answering. *In* Jianwen Su, editor, *Proceedings of the 28th Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'09), Providence, Rhode Island, USA, June-July 2009*, pages 237–246. ACM Press.

(CI-245) Mathieu Baudet, Véronique Cortier, and Stéphanie Delaune. YAPA : A generic tool for computing intruder knowledge. *In* Ralf Treinen, editor, *Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09), Brasília, Brazil, June-July 2009*, volume 5595 of *Lecture Notes in Computer Science*, pages 148–163. Springer.

(CI-246) Marco Beccuti, Giuliana Franceschinis, Daniele Codetta-Raiteri, and Serge Haddad. Parametric NdRFT for the derivation of optimal repair strategies. *In Proceedings of the 39th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'09), Estoril, Portugal, June-July 2009*, pages 399–408. IEEE Computer Society Press.

(CI-247) Anne Bouillard, Sidney Rosario, Albert Benveniste, and Stefan Haar. Monotonicity in service orchestrations. *In* Giuliana Franceschinis and Karsten Wolf, editors, *Proceedings of the 30th International Conference on Applications and Theory of Petri Nets (ICATPN'09), Paris, France, June 2009*, volume 5606 of *Lecture Notes in Computer Science*, pages 263–282. Springer.

(CI-248) Sergiu Bursuc and Hubert Comon-Lundh. Protocol security and algebraic properties : decision results for a bounded number of sessions. *In* Ralf Treinen, editor, *Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09), Brasília, Brazil, June-July 2009*, volume 5595 of *Lecture Notes in Computer Science*, pages 133–147. Springer.

(CI-249) Rohit Chadha, Stéphanie Delaune, and Steve Kremer. Epistemic logic for the applied pi calculus. *In* David Lee, Antónia Lopes, and Arnd Poetzsch-Heffter, editors, *Proceedings of IFIP International Conference on Formal Techniques for Distributed Systems (FMOODS/FORTE'09), Lisbon, Portugal, June 2009*, volume 5522 of *Lecture Notes in Computer Science*, pages 182–197. Springer.

(CI-250) Diego Figueira. Satisfiability of downward XPath with data equality tests. *In* Jianwen Su, editor, *Proceedings of the 28th Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'09), Providence, Rhode Island, USA, June-July 2009*, pages 197–206. ACM Press.

(CI-251) Guillem Godoy and Florent Jacquemard. Unique normalization for shallow TRS. *In* Ralf Treinen, editor, *Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09), Brasília, Brazil, June-July 2009*, volume 5595 of *Lecture Notes in Computer Science*, pages 63–77. Springer.

(CI-252) Serge Haddad, Fabrice Kordon, Laure Petrucci, Jean-François Pradat-Peyre, and Nicolas Trèves. Efficient state-based analysis by introducing bags in Petri nets color domains. *In Proceedings of the 28th American Control Conference (ACC'09), Saint Louis, Missouri, USA, June 2009*, pages 5018–5025.

(CI-253) Elie Bursztein. Extending anticipation games with location, penalty and timeline. *In* Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli, editors, *Revised Selected Papers of the 5th International Workshop on Formal Aspects in Security and Trust (FAST'08), Malaga, Spain, October 2008*, volume 5491 of *Lecture Notes in Computer Science*, pages 272–286. Springer, April 2009.

(CI-254) Adrià Gascón, Guillem Godoy, and Florent Jacquemard. Closure of tree automata languages under innermost rewriting. *In* Aart Middeldorp, editor, *Proceedings of the 8th International Workshop on Reduction Strategies in Rewriting and Programming (WRS'08), Castle of Hagenberg, Austria, July 2008*, volume 237 of *Electronic Notes in Theoretical Computer Science*, pages 23–38. Elsevier Science Publishers, April 2009.

(CI-255) Florent Jacquemard, Francis Klay, and Camille Vacher. Rigid tree automata. *In* Adrian Horia Dediu, Armand Mihai Ionescu, and Carlos Martín-Vide, editors, *Proceedings of the 3rd International Conference on Language and Automata Theory and Applications (LATA'09), Tarragona, Spain, April 2009*, volume 5457 of *Lecture Notes in Computer Science*, pages 446–457. Springer.

(CI-256) Serge Abiteboul, Pierre Bourhis, and Bogdan Marinoiu. Efficient maintenance techniques for views over active documents. *In* Martin L. Kersten, Boris Novikov, Jens Teubner, Vladimir Polutin, and Stefan Manegold, editors, *Advances in Database Technology — Proceedings of the 12th International Conference on Extending Database Technology (EDBT'09), Saint Petersburg, Russia, March 2009*, ACM International Conference Proceeding Series, pages 1076–1087. Springer.

(CI-257) Serge Abiteboul, Ohad Greenshpan, Tova Milo, and Neoklis Polyzotis. MatchUp : Autocompletion for mashups. *In* Yannis E. Ioannidis, Dik Lun Lee, and Raymond T. Ng, editors, *Proceedings of the 25th International Conference on Data Engineering (ICDE'09), Shanghai, China, March-April 2009*, pages 1479–1482. IEEE Computer Society Press.

(CI-258) Kshitij Bansal, Rémi Brochenin, and Étienne Lozes. Beyond shapes : Lists with ordered data. *In* Luca de Alfaro, editor, *Proceedings of the 12th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'09), York, UK, March 2009*, volume 5504 of *Lecture Notes in Computer Science*, pages 425–439. Springer.

(CI-259) Béatrice Bérard and Serge Haddad. Interrupt timed automata. *In* Luca de Alfaro, editor, *Proceedings of the 12th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'09), York, UK, March 2009*, volume 5504 of *Lecture Notes in Computer Science*, pages 197–211. Springer.

(CI-260) Dietmar Berwanger, Krishnendu Chatterjee, Martin De Wulf, Laurent Doyen, and Thomas A. Henzinger. Alpaga : A tool for solving parity games with imperfect information. *In* Stefan Kowalewski and Anna Philippou, editors, *Proceedings of the 15th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'09), York, UK, March 2009*, volume 5505 of *Lecture Notes in Computer Science*, pages 58–61. Springer.

(CI-261) Benedikt Bollig, Manuela-Lidia Grindei, and Peter Habermehl. Realizability of concurrent recursive programs. *In* Luca de Alfaro, editor, *Proceedings of the 12th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'09), York, UK, March 2009*, volume 5504 of *Lecture Notes in Computer Science*, pages 410–424. Springer.

(CI-262) Alain Finkel and Jean Goubault-Larrecq. Forward analysis for WSTS, part I : Completions. *In* Susanne Albers and Jean-Yves Marion, editors, *Proceedings of the 26th Annual Symposium on Theoretical Aspects of Computer Science (STACS'09), Freiburg, Germany, February 2009*, volume 3 of *Leibniz International Proceedings in Informatics*, pages 433–444. Leibniz-Zentrum für Informatik.

(CI-263) Thomas Brihaye, Arnaud Da Costa, François Laroussinie, and Nicolas Markey. ATL with strategy contexts and bounded memory. *In* Sergei N. Artemov and Anil Nerode, editors, *Proceedings of the Symposium on Logical Foundations of Computer Science (LFCS'09), Deerfield Beach, Florida, USA, January 2009*, volume 5407 of *Lecture Notes in Computer Science*, pages 92–106. Springer.

(CI-264) Thomas Chatain, Paul Gastin, and Nathalie Sznajder. Natural specifications yield decidability for distributed synthesis of asynchronous systems. *In* Mogens Nielsen, Antonín Kučera, Peter Bro Miltersen, Catuscia Palamidessi, Petr Tůma, and Franck Valencia, editors, *Proceedings of the 35th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'09), Špindlerův Mlýn, Czech Republic, January 2009*, volume 5404 of *Lecture Notes in Computer Science*, pages 141–152. Springer.

(CI-265) Étienne André, Thomas Chatain, Emmanuelle Encrenaz, and Laurent Fribourg. An inverse method for parametric timed automata. *In* Vesa Halava and Igor Potapov, editors, *Proceedings of the 2nd*

Workshop on Reachability Problems in Computational Models (RP'08), Liverpool, UK, September 2008, volume 223 of *Electronic Notes in Theoretical Computer Science*, pages 29–46. Elsevier Science Publishers, December 2008.

(CI-266) Myrto Arapinis, Stéphanie Delaune, and Steve Kremer. From one session to many : Dynamic tags for security protocols. *In* Iliano Cervesato, Helmut Veith, and Andrei Voronkov, editors, *Proceedings of the 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'08), Doha, Qatar, November 2008*, volume 5330 of *Lecture Notes in Artificial Intelligence*, pages 128–142. Springer.

(CI-267) Serge Abiteboul, Ohad Greenshpan, and Tova Milo. Modeling the mashup space. *In* Chee Yong Chan and Neoklis Polyzotis, editors, *Proceedings of the 10th ACM International Workshop on Web Information and Data Management (WIDM'08), Napa Valley, California, USA, October 2008*, pages 87–94. ACM Press.

(CI-268) Marco Beccuti, Daniele Codetta-Raiteri, Giuliana Franceschinis, and Serge Haddad. Non deterministic repairable fault trees for computing optimal repair strategy. *In* Tijani Chahed, Stavros Toumpis, and Uri Yechiali, editors, *Proceedings of the 3rd International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS'08), Athens, Greece, October 2008*. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering.

(CI-269) Hubert Comon-Lundh and Véronique Cortier. Computational soundness of observational equivalence. *In Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS'08), Alexandria, Virginia, USA, October 2008*, pages 109–118. ACM Press.

(CI-270) Mohamed Faouzi Atig, Benedikt Bollig, and Peter Habermehl. Emptiness of multi-pushdown automata is 2ETIME-complete. *In* Masami Ito and Masafumi Toyama, editors, *Proceedings of the 12th International Conference on Developments in Language Theory (DLT'08), Kyoto, Japan, September 2008*, volume 5257 of *Lecture Notes in Computer Science*, pages 121–133. Springer.

(CI-271) Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Nicolas Markey. Quantitative model-checking of one-clock timed automata under probabilistic semantics. *In Proceedings of the 5th International Conference on Quantitative Evaluation of Systems (QEST'08), Saint Malo, France, September 2008*, pages 55–64. IEEE Computer Society Press.

(CI-272) Patricia Bouyer, Thomas Brihaye, Marcin Jurdziński, Ranko Lazić, and Michał Rutkowski. Average-price and reachability-price games on hybrid automata with strong resets. *In* Franck Cassez and Claude Jard, editors, *Proceedings of the 6th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'08), Saint-Malo, France, September 2008*, volume 5215 of *Lecture Notes in Computer Science*, pages 63–77. Springer.

(CI-273) Patricia Bouyer, Uli Fahrenberg, Kim G. Larsen, Nicolas Markey, and Jiří Srba. Infinite runs in weighted timed automata with energy constraints. *In* Franck Cassez and Claude Jard, editors, *Proceedings of the 6th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'08), Saint-Malo, France, September 2008*, volume 5215 of *Lecture Notes in Computer Science*, pages 33–47. Springer.

(CI-274) Rémi Brochenin, Stéphane Demri, and Étienne Lozes. On the almighty wand. *In* Michael Kaminski and Simone Martini, editors, *Proceedings of the 17th Annual EACSL Conference on Computer Science Logic (CSL'08), Bertinoro, Italy, September 2008*, volume 5213 of *Lecture Notes in Computer Science*, pages 323–338. Springer.

(CI-275) Najla Chamseddine, Marie Duflot, Laurent Fribourg, Claudine Picaronny, and Jeremy Sproston. Computing expected absorption times for parametric determinate probabilistic timed automata. *In Proceedings of the 5th International Conference on Quantitative Evaluation of Systems (QEST'08), Saint Malo, France, September 2008*, pages 254–263. IEEE Computer Society Press.

(CI-276) Thomas Place. Characterization of logics over ranked tree languages. *In* Michael Kaminski and Simone Martini, editors, *Proceedings of the 17th Annual EACSL Conference on Computer Science Logic (CSL'08), Bertinoro, Italy, September 2008*, volume 5213 of *Lecture Notes in Computer Science*, pages 401–415. Springer.

(CI-277) Serge Abiteboul, Tristan Allard, Philippe Chatalic, Georges Gardarin, Anca Ghitescu, François Goasdoué, Ioana Manolescu, Benjamin Nguyen, Mohamed Ouazara, Aditya Somani, Nicolas Travers, Gabriel Vasile, and Spyros Zoupanos. WebContent : efficient P2P warehousing of web data. *In* Gerald Weber, editor, *Proceedings of the 34th International Conference on Very Large Data Bases (VLDB'08), Auckland, New Zealand, August 2008*, volume 1 of *Proceedings of the VLDB Endowment*, pages 1428–1431. ACM Press.

(CI-278) S. Akshay, Benedikt Bollig, Paul Gastin, Madhavan Mukund, and K. Narayan Kumar. Distributed timed automata with independently evolving clocks. *In* Franck van Breugel and Marsha Chechik, editors, *Proceedings of the 19th International Conference on Concurrency Theory (CONCUR'08), Toronto, Canada, August 2008*, volume 5201 of *Lecture Notes in Computer Science*, pages 82–97. Springer.

(CI-279) Paolo Baldan, Thomas Chatain, Stefan Haar, and Barbara König. Unfolding-based diagnosis of systems with an evolving topology. *In* Franck van Breugel and Marsha Chechik, editors, *Proceedings of the 19th International Conference on Concurrency Theory (CONCUR'08), Toronto, Canada, August 2008*, volume 5201 of *Lecture Notes in Computer Science*, pages 203–217. Springer.

(CI-280) Adel Bouhoula and Florent Jacquemard. Automated induction with constrained tree automata. *In* Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *Proceedings of the 4th International Joint Conference on Automated Reasoning (IJCAR'08), Sydney, Australia, August 2008*, volume 5195 of *Lecture Notes in Artificial Intelligence*, pages 539–553. Springer-Verlag.

(CI-281) Pierre Chambart and Philippe Schnoebelen. Mixing lossy and perfect fifo channels. *In* Franck van Breugel and Marsha Chechik, editors, *Proceedings of the 19th International Conference on Concurrency Theory (CONCUR'08), Toronto, Canada, August 2008*, volume 5201 of *Lecture Notes in Computer Science*, pages 340–355. Springer.

(CI-282) Alain Finkel and Arnaud Sangnier. Reversal-bounded counter machines revisited. *In* Edward Ochmański and Jerzy Tyszkiewicz, editors, *Proceedings of the 33rd International Symposium on Mathematical Foundations of Computer Science (MFCS'08), Toruń, Poland, August 2008*, volume 5162 of *Lecture Notes in Computer Science*, pages 323–334. Springer.

(CI-283) Steve Kremer, Antoine Mercier, and Ralf Treinen. Proving group protocols secure against eavesdroppers. *In* Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *Proceedings of the 4th International Joint Conference on Automated Reasoning (IJCAR'08), Sydney, Australia, August 2008*, volume 5195 of *Lecture Notes in Artificial Intelligence*, pages 116–131. Springer-Verlag.

(CI-284) Étienne Lozes and Jules Villard. A spatial equational logic for the applied π-calculus. *In* Franck van Breugel and Marsha Chechik, editors, *Proceedings of the 19th International Conference on Concurrency Theory (CONCUR'08), Toronto, Canada, August 2008*, volume 5201 of *Lecture Notes in Computer Science*, pages 387–401. Springer.

(CI-285) Serge Abiteboul, Ioana Manolescu, and Spyros Zoupanos. OptimAX : Optimizing distributed ActiveXML applications. *In* Daniel Schwabe, Francisco Curbera, and Paul Dantzig, editors, *Proceedings of the 8th International Conference on Web Engineering (ICWE'08), Yorktown Heights, New York, USA, July 2008*, pages 299–310. IEEE Computer Society Press.

(CI-286) Carlos Areces, Diego Figueira, Santiago Figueira, and Sergio Mera. Expressive power and decidability for memory logics. *In* Wilfrid Hodges and Ruy de Queiroz, editors, *Proceedings of the 15th Workshop on Logic, Language, Information and Computation (WoLLIC'08), Edinburgh, Scotland, UK, July 2008*, volume 5110 of *Lecture Notes in Computer Science*, pages 56–68. Springer.

(CI-287) Mikołaj Bojańczyk and Luc Segoufin. Tree languages defined in first-order logic with one quantifier alternation. *In* Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP'08) – Part II, Reykjavik, Iceland, July 2008*, volume 5126 of *Lecture Notes in Computer Science*, pages 233–245. Springer.

(CI-288) Ahmed Bouajjani, Peter Habermehl, Lukáš Holík, Tayssir Touili, and Tomáš Vojnar. Antichain-based universality and inclusion testing over nondeterministic finite tree automata. *In* Oscar H. Ibarra and Bala Ravikumar, editors, *Proceedings of the 13th International Conference on Implementation* *and Application of Automata (CIAA'08), San Francisco, California, USA, July 2008*, volume 5148 of *Lecture Notes in Computer Science*, pages 57–67. Springer-Verlag.

(CI-289) Patricia Bouyer, Nicolas Markey, Joël Ouaknine, and James Worrell. On expressiveness and complexity in real-time model checking. *In* Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP'08) – Part II, Reykjavik, Iceland, July 2008*, volume 5126 of *Lecture Notes in Computer Science*, pages 124–135. Springer.

(CI-290) Serge Haddad, Lynda Mokdad, and Samir Youcef. Response time analysis of composite web services. *In Proceedings of the 6th Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP'08), Graz, Austria, July 2008*, pages 506–510. IEEE Computer Society Press.

(CI-291) Florent Jacquemard and Michaël Rusinowitch. Closure of Hedge-automata languages by Hedge rewriting. *In* Andrei Voronkov, editor, *Proceedings of the 19th International Conference on Rewriting Techniques and Applications (RTA'08), Hagenberg, Austria, July 2008*, volume 5117 of *Lecture Notes in Computer Science*, pages 157–171. Springer.

(CI-292) Serge Abiteboul, Luc Segoufin, and Victor Vianu. Static analysis of active XML systems. *In* Maurizio Lenzerini and Domenico Lembo, editors, *Proceedings of the 27th Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'08), Vancouver, Canada, June 2008*, pages 221–230. ACM Press.

(CI-293) Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Marcus Größer. Almost-sure model checking of infinite paths in one-clock timed automata. *In Proceedings of the 23rd Annual IEEE Symposium on Logic in Computer Science (LICS'08), Pittsburgh, Pennsylvania, USA, June 2008*, pages 217–226. IEEE Computer Society Press.

(CI-294) Mikołaj Bojańczyk, Luc Segoufin, and Howard Straubing. Piecewise testable tree languages. *In Proceedings of the 23rd Annual IEEE Symposium on Logic in Computer Science (LICS'08), Pittsburgh, Pennsylvania, USA, June 2008*, pages 442–451. IEEE Computer Society Press.

(CI-295) Florent Bouchy, Alain Finkel, and Jérôme Leroux. Decomposition of decidable first-order logics over integers and reals. *In Proceedings of the 15th International Symposium on Temporal Representation and Reasoning (TIME'08), Montréal, Canada, June 2008*, pages 147–155. IEEE Computer Society Press.

(CI-296) Thomas Brihaye, Mohamed Ghannem, Nicolas Markey, and Lionel Rieg. Good friends are hard to find ! *In Proceedings of the 15th International Symposium on Temporal Representation and Reasoning (TIME'08), Montréal, Canada, June 2008*, pages 32–40. IEEE Computer Society Press.

(CI-297) Pierre Chambart and Philippe Schnoebelen. The ordinal recursive complexity of lossy channel systems. *In Proceedings of the 23rd Annual IEEE Symposium on Logic in Computer Science (LICS'08), Pittsburgh, Pennsylvania, USA, June 2008*, pages 205–216. IEEE Computer Society Press.

(CI-298) Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Composition of password-based protocols. *In Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08), Pittsburgh, Pennsylvania, USA, June 2008*, pages 239–251. IEEE Computer Society Press.

(CI-299) Stéphanie Delaune, Steve Kremer, and Graham Steel. Formal analysis of PKCS#11. *In Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08), Pittsburgh, Pennsylvania, USA, June 2008*, pages 331–344. IEEE Computer Society Press.

(CI-300) Stéphanie Delaune, Mark D. Ryan, and Ben Smyth. Automatic verification of privacy properties in the applied pi-calculus. *In* Yuecel Karabulut, John Mitchell, Peter Herrmann, and Christian Damsgaard Jensen, editors, *Proceedings of the 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM'08), Trondheim, Norway, June 2008*, volume 263 of *IFIP Conference Proceedings*, pages 263–278. Springer.

(CI-301) Jean Goubault-Larrecq. Towards producing formally checkable security proofs, automatically. *In Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08), Pittsburgh, Pennsylvania, USA, June 2008*, pages 224–238. IEEE Computer Society Press.

(CI-302) Balder ten Cate and Luc Segoufin. XPath, transitive closure logic, and nested tree walking automata. *In* Maurizio Lenzerini and Domenico Lembo, editors, *Proceedings of the 27th Annual ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (PODS'08), Vancouver, Canada, June 2008*, pages 251–260. ACM Press.

(CI-303) Béatrice Bérard, Serge Haddad, Lom Messan Hillah, Fabrice Kordon, and Yann Thierry-Mieg. Collision avoidance in intelligent transport systems : Towards an application of control theory. *In Proceedings of the 9th Workshop on Discrete Event Systems (WODES'08), Gothenburg, Sweden, May 2008*, pages 346–351.

(CI-304) Elie Bursztein. Probabilistic protocol identification for hard to classify protocol. *In* Jose A. Onieva, Damien Sauveron, Serge Chaumette, Dieter Gollmann, and Konstantinos Markantonakis, editors, *Proceedings of the 2nd International Workshop on Information Security Theory and Practices (WISTP'08), Sevilla, Spain, May 2008*, volume 5019 of *Lecture Notes in Computer Science*, pages 49–63. Springer. Best paper award.

(CI-305) Serge Abiteboul, Ioana Manolescu, Nicoleta Polyzotis, Neoklis amd Preda, and Chong Sun. XML processing in DHT networks. *In* Gustavo Alonso, José A. Blakeley, and Arbee L. P. Chen, editors, *Proceedings of the 24th International Conference on Data Engineering (ICDE'08), Cancun, Mexico, April 2008*, pages 606–615. IEEE Computer Society Press.

(CI-306) Serge Abiteboul, Ioana Manolescu, and Spyros Zoupanos. OptimAX : efficient support for data-intensive mash-ups. *In* Gustavo Alonso, José A. Blakeley, and Arbee L. P. Chen, editors, *Proceedings of the 24th International Conference on Data Engineering (ICDE'08), Cancun, Mexico, April 2008*, pages 1564–1567. IEEE Computer Society Press.

(CI-307) Serge Abiteboul, Bogdan Marinoiu, and Pierre Bourhis. Distributed monitoring of peer-to-peer systems. *In* Gustavo Alonso, José A. Blakeley, and Arbee L. P. Chen, editors, *Proceedings of the 24th International Conference on Data Engineering (ICDE'08), Cancun, Mexico, April 2008*, pages 1572–1575. IEEE Computer Society Press.

(CI-308) Emmanuelle Encrenaz and Laurent Fribourg. Time separation of events : An inverse method. *In* Catuscia Palamidessi and Franck Valencia, editors, *Proceedings of the LIX Colloquium on Emerging Trends in Concurrency Theory (LIX'06), Palaiseau, France, November 2006*, volume 209 of *Electronic Notes in Theoretical Computer Science*, pages 135–148. Elsevier Science Publishers, April 2008.

(CI-309) Patricia Bouyer, Nicolas Markey, and Pierre-Alain Reynier. Robust analysis of timed automata *via* channel machines. *In* Roberto Amadio, editor, *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March-April 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 157–171. Springer.

(CI-310) Pierre Chambart and Philippe Schnoebelen. The ω-regular Post embedding problem. *In* Roberto Amadio, editor, *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March-April 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 97–111. Springer.

(CI-311) Stéphane Demri, Ranko Lazić, and Arnaud Sangnier. Model checking freeze LTL over one-counter automata. *In* Roberto Amadio, editor, *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March-April 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 490–504. Springer.

(CI-312) Jean Goubault-Larrecq. Prevision domains and convex powercones. *In* Roberto Amadio, editor, *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March-April 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 318–333. Springer.

(CI-313) Jean Goubault-Larrecq. Simulation hemi-metrics between infinite-state stochastic games. *In* Roberto Amadio, editor, *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March-April 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 50–65. Springer.

(CI-314) Peter Habermehl, Radu Iosif, and Tomáš Vojnar. What else is decidable about arrays ? *In* Roberto Amadio, editor, *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March-April 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 474–489. Springer.

(CI-315) Patricia Bouyer, Nicolas Markey, Joël Ouaknine, Philippe Schnoebelen, and James Worrell. On termination for faulty channel machines. *In* Susanne Albers and Pascal Weil, editors, *Proceedings of the 25th Annual Symposium on Theoretical Aspects of Computer Science (STACS'08), Bordeaux, France, February 2008*, volume 1 of *Leibniz International Proceedings in Informatics*, pages 121–132. Leibniz-Zentrum für Informatik.

(CI-316) Vincent Bernat and Hubert Comon-Lundh. Normal proofs in intruder theories. *In* Mitsu Okada and Ichiro Satoh, editors, *Revised Selected Papers of the 11th Asian Computing Science Conference (ASIAN'06), Tokyo, Japan, December 2006*, volume 4435 of *Lecture Notes in Computer Science*, pages 151–166. Springer, January 2008.

Autres conférences

(CO-1) Diego V. Simões De Sousa, Henrique Viana, Nicolas Markey, and Jose Antônio F. de Macêdo. Querying trajectories through model checking based on timed automata. *In* Marco A. Casanova, editor, *Proceedings of the 27th Brazilian Symposium on Databases (SBBD'12), São Paulo, Brazil, October 2012*. Sociedade Brasileira de Computação.

(CO-2) Roxanne Saint Bauzel and Alain Finkel. Qu'est-ce qu'une représentation efficace pour favoriser les apprentissages ? *In Actes du 54ème Congrès National de la Société Française de Psychologie (SFP'12), Montpellier, France, September 2012*, pages 89–91.

(CO-3) Claire Gardent, Guy Perrier, Yannick Parmentier, and Sylvain Schmitz. Lexical disambiguation in LTAG using left context. *In Proceedings of the 5th Language & Technology Conference (LTC'11), Poznań, Poland, November 2011*.

(CO-4) Krishnendu Chatterjee and Laurent Doyen. Games and markov decision processes with mean-payoff parity and energy parity objectives. *In* Jan Bouda, Ivana Černá, Lukáš Sekanina, and Tomáš Vojnar, editors, *Proceedings of the 7th Annual Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS'11), Lednice, Czech Republic, October 2011*, volume 7119 of *Lecture Notes in Computer Science*. Springer.

(CO-5) Roxanne Saint Bauzel and Alain Finkel. Se représenter pour mieux apprendre : les représentations mentales comme outils didactiques favorisant la transmission du savoir. *In Actes du 53ème Congrès National de la Société Française de Psychologie (SFP'11), Metz, France, September 2011*, pages 171–173.

(CO-6) Ştefan Ciobâcă. Computing finite variants for subterm convergent rewrite systems. *In* Franz Baader, editor, *Proceedings of the 25th International Workshop on Unification (UNIF'11), Wrocław, Poland, July 2011*.

(CO-7) Sylvain Schmitz. A note on sequential rule-based POS tagging. *In* Andreas Maletti, editor, *Proceedings of the 9th International Workshop on Finite-State Methods and Natural Language Processing (FSMNLP'11), Blois, France, July 2011*, pages 83–87. ACL Press.

(CO-8) Hedi Benzina. Logic in virtualized systems. *In Proceedings of the International Conference on Computer Applications and Network Security (ICCANS'11), Republic of Maldives, May 2011*.

(CO-9) Laurent Doyen, Thierry Massart, and Mahsa Shirmohammadi. Synchronizing objectives for Markov decision processes. *In* Johannes Reich and Bernd Finkbeiner, editors, *Proceedings of the International Workshop on Interactions, Games and Protocols (iWIGP'11), Saarbrücken, Germany, March 2011*, volume 50 of *Electronic Proceedings in Theoretical Computer Science*, pages 61–75.

(CO-10) H. Mahdi Zargayouna, Flavien Balbo, and Serge Haddad. Agents secure interaction in data driven languages. *In* Mehdi Dastani, Amal El Fallah Seghrouchni, João Leite, and Paolo Torroni, editors, *Revised Selected Papers of the 2nd Workshop on LAnguages, methodologies and Development tools for multi-agent systemS (LADS'09), Torino, Italy, September 2009*, volume 6039 of *Lecture Notes in Computer Science*, pages 72–91. Springer, 2010.

(CO-11) Hedi Benzina and Jean Goubault-Larrecq. Some ideas on virtualized systems security, and monitors. *In* Ana Cavalli and Jean Leneutre, editors, *Revised Selected Papers of the 5th International Workshop on Data Privacy Management and Autonomous Spontaneous Security (DPM'10) and 3rd International Workshop on Autonomous and Spontaneous Security (SETOP'10), Athens, Greece, September 2010*, volume 6514 of *Lecture Notes in Computer Science*, pages 244–258. Springer.

(CO-12) Olivier Bouissou, Éric Goubault, Jean Goubault-Larrecq, and Sylvie Putot. A generalization of P-boxes to affine arithmetic, and applications to static analysis of programs. *In Proceedings of the 14th GAMM-IMACS International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics (SCAN'10), Lyon, France, September 2010*.

(CO-13) Ana Bušić, Hilal Djafri, and Jean-Michel Fourneau. Stochastic bounds for censored Markov chains. *In* Michele Benzi and Tugrul Dayar, editors, *Proceedings of the 6th International Meeting on the Numerical Solution of Markov Chain (NSMC'10), Williamsburg, Virginia, USA, September 2010*.

(CO-14) Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel. A formal analysis of authentication in the TPM (short paper). *In* Véronique Cortier and Kostas Chatzikokolakis, editors, *Preliminary Proceedings of the 8th International Workshop on Security Issues in Coordination Models, Languages and Systems (SecCo'10), Paris, France, August 2010*.

(CO-15) Aiswarya Cyriac. A new version of focus games for LTL satisfiability. *In Proceedings of the Workshop on Comparing Logical Decision Methods (CLoDeM'10), Edinburgh, Scotland, UK, July 2010*.

(CO-16) Morten Dahl, Stéphanie Delaune, and Graham Steel. Formal analysis of privacy for vehicular mix-zones. *In* Véronique Cortier, Mark D. Ryan, and Vitaly Shmatikov, editors, *Proceedings of the Workshop on Foundations of Security and Privacy (FCS-PrivMod'10), Edinburgh, Scotland, UK, July 2010*.

(CO-17) Laurent Doyen, Thomas A. Henzinger, Axel Legay, and Dejan Nickovic. Robustness of sequential circuits. *In* Luís Gomes and Victor Khomenko, editors, *Proceedings of the 10th International Conference on Application of Concurrency to System Design (ACSD'10), Braga, Portugal, June 2010*, pages 978–0–7695–4066–5. IEEE Computer Society Press.

(CO-18) Dorsaf El Hog-Benzina, Serge Haddad, and Rolf Hennicker. Process refinement and asynchronous composition with modalities. *In* Natalia Sidorova and Alexander Serebrenik, editors, *Proceedings of the 2nd International Workshop on Abstractions for Petri Nets and Other Models of Concurrency (APNOC'10), Braga, Portugal, June 2010*.

(CO-19) Thomas Chatain and Claude Jard. Sémantique concurrente symbolique des réseaux de Petri saufs et dépliages finis des réseaux temporels. *In Actes de la 10ème Conférence Internationale sur les NOuvelles TEchnologies de la RÉpartition (NOTERE'10), Tozeur, Tunisia, May-June 2010*. IEEE Computer Society Press.

(CO-20) Étienne André, Thomas Chatain, Olivier De Smet, Laurent Fribourg, and Silvain Ruel. Synthèse de contraintes temporisées pour une architecture d'automatisation en réseau. *In* Didier Lime and Olivier H. Roux, editors, *Actes du 7ème Colloque sur la Modélisation des Systèmes Réactifs (MSR'09), Nantes, France, November 2009*, volume 43(7-9) of *Journal Européen des Systèmes Automatisés*, pages 1049–1064. Hermès.

(CO-21) Serge Haddad, Lynda Mokdad, and Samir Youcef. Bornes du temps de réponse des services web composites. *In* Didier Lime and Olivier H. Roux, editors, *Actes du 7ème Colloque sur la Modélisation des Systèmes Réactifs (MSR'09), Nantes, France, November 2009*, volume 43(7-9) of *Journal Européen des Systèmes Automatisés*, pages 969–983. Hermès.

(CO-22) Ben Smyth, Mark D. Ryan, Steve Kremer, and Mounira Kourjieh. Election verifiability in electronic voting protocols (preliminary version). *In* Olivier Pereira, Jean-Jacques Quisquater, and François-Xavier Standaert, editors, *Proceedings of the 4th Benelux Workshop on Information and System Security (WISSEC'09), Louvain-la-Neuve, Belgium, November 2009*.

(CO-23) Graham Steel. Towards a formal analysis of the SeVeCoM API. *In* Christof Paar and Thomas Wollinger, editors, *Proceedings of the 7th Conference on Embedded Security in Cars (ESCAR'09), Düsseldorf, Germany, November 2009*.

(CO-24) Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. A decision procedure for proving observational equivalence. *In* Michele Boreale and Steve Kremer, editors, *Preliminary Proceedings of the 7th International Workshop on Security Issues in Coordination Models, Languages and Systems (SecCo'09), Bologna, Italy, October 2009*.

(CO-25) Étienne André. Une méthode inverse pour les plus courts chemins. *In Actes de la 6ème École Temps-Réel (ETR'09), Paris, France, September 2009*.

(CO-26) Thomas Chatain, Alexandre David, and Kim G. Larsen. Playing games with timed games. *In* Alessandro Giua, Manuel Silva, and Janan Zaytoon, editors, *Proceedings of the 3rd IFAC Conference on Analysis and Design of Hybrid Systems (ADHS'09), Zaragoza, Spain, September 2009*.

(CO-27) Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Modeling and verifying ad hoc routing protocol. *In* Hubert Comon-Lundh and Catherine Meadows, editors, *Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, New York, USA, July 2009*, pages 33–46.

(CO-28) Ştefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. Computing knowledge in security protocols under convergent equational theories. *In* Hubert Comon-Lundh and Catherine Meadows, editors, *Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, New York, USA, July 2009*, pages 47–58.

(CO-29) Steve Kremer, Antoine Mercier, and Ralf Treinen. Reducing equational theories for the decision of static equivalence (preliminary version). *In* Hubert Comon-Lundh and Catherine Meadows, editors, *Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, New York, USA, July 2009*.

(CO-30) Graham Steel. Computational soundness for APIs. *In* Ralf Küsters, editor, *Proceedings of the 5th Workshop on Formal and Computational Cryptography (FCC'09), Port Jefferson, New York, USA, July 2009*.

(CO-31) Elie Bursztein. NetQi : A model checker for anticipation game. *In* Sungdeok Cha, Jin-Young Choi, Moonzoo Kim, Insup Lee, and Mahesh Viswanathan, editors, *Proceedings of the 6th International Symposium on Automated Technology for Verification and Analysis (ATVA'08), Seoul, Korea, October 2008*, volume 5311 of *Lecture Notes in Computer Science*, pages 246–251. Springer.

(CO-32) Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, and Martin Leucker. *Smyle* : A tool for synthesizing distributed models from scenarios by learning. *In* Franck van Breugel and Marsha Chechik, editors, *Proceedings of the 19th International Conference on Concurrency Theory (CONCUR'08), Toronto, Canada, August 2008*, volume 5201 of *Lecture Notes in Computer Science*, pages 162–166. Springer.

(CO-33) Pierre Arnoux and Alain Finkel. Using mental imagery processes for teaching/searching in mathematics and computer science. *In Proceedings of the 11th International Congress on Mathematical Education (ICME'08), Monterrey, Mexico, July 2008*.

(CO-34) Sławomir Lasota, David Nowak, and Zhang Yu. On completeness of logical relations for monadic types. *In* Mitsu Okada and Ichiro Satoh, editors, *Revised Selected Papers of the 11th Asian Computing Science Conference (ASIAN'06), Tokyo, Japan, December 2006*, volume 4435 of *Lecture Notes in Computer Science*, pages 223–230. Springer, January 2008.

Thèses

(TH-1) Ocan Sankur. Robustness in timed automata : Analysis, synthesis, implementation. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2013.

(TH-2) Rémi Bonnet. Theory of well-structured transition systems and extended vector-addition systems. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, January 2013.

(TH-3) Sandie Balaguer. La concurrence dans les systèmes distribués temps-réel. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012.

(TH-4) Hedi Benzina. Enforcing virtualized systems security. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012.

(TH-5) Vincent Cheval. Automatic verification of cryptographic protocols : privacy-type properties. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012.

(TH-6) Romain Brenguier. Équilibres de Nash dans les jeux concurrents – Application aux jeux temporisés. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2012.

(TH-7) Étienne Lozes. Separation logic : Expressiveness and copyless message-passing. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, July 2012.

(TH-8) Hilal Djafri. Approches numériques et statistiques pour le model checking des processus stochastiques. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2012.

(TH-9) Laurent Doyen. Games and automata : From boolean to quantitative verification. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, March 2012.

(TH-10) Mathilde Arnaud. Formal verification of secured routing protocols. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2011.

(TH-11) Ştefan Ciobâcă. Automated verification of security protocols with appplications to electronic voting. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2011.

(TH-12) Florent Jacquemard. Extended tree automata for the verification of infinite state systems. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, November 2011.

(TH-13) Pierre Chambart. Du problème de sous-mot de Post et de la complexité des canaux non fiables. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2011.

(TH-14) Arnaud Da Costa. Propriétés de jeux multi-agents. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2011.

(TH-15) Alban Galland. Distributed data management with access control. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2011.

(TH-16) Nicolas Markey. Verification of embedded systems – algorithms and complexity. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, April 2011.

(TH-17) Stéphanie Delaune. Verification of security protocols : from confidentiality to privacy. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, March 2011.

(TH-18) Steve Kremer. Modelling and analyzing security protocols in cryptographic process calculi. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, March 2011.

(TH-19) Graham Steel. Formal analysis of security APIs. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, March 2011.

(TH-20) Pierre Bourhis. On the dynamics of active documents for distributed data management. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2011.

(TH-21) Jules Villard. Heaps and hops. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2011.

(TH-22) Étienne André. An inverse method for the synthesis of timing parameters in concurrent systems. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2010.

(TH-23) Diego Figueira. On decidable automata on data words and data trees in relation to satisfiability of LTL and XPath. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2010.

(TH-24) Thomas Place. Decidable characterizations for tree logics. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2010.

(TH-25) Camille Vacher. Automates à contraintes globales pour la vérification de propriétés de sécurité. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2010.

(TH-26) S. Akshay. Spécification et vérification pour des systèmes distribués et temporisés. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2010.

(TH-27) Jean-Loup Carré. Analyse statique de programmes multi-thread pour l'embarqué. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2010.

(TH-28) Sergiu Bursuc. Contraintes de déductibilité dans une algèbre quotient : réduction de modèles et applications à la sécurité. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2009.

(TH-29) Antoine Mercier. Contributions à l'analyse automatique des protocoles cryptographiques en présence de propriétés algébriques : protocoles de groupe, équivalence statique. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2009.

(TH-30) Florent Bouchy. Logiques et modèles pour la vérification de systèmes infinis. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2009.

(TH-31) Nathalie Sznajder. Synthèse de systèmes distribués ouverts. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2009.

(TH-32) Najla Chamseddine. Analyse quantitative parametrée d'automates temporisés probabilistes. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2009.

(TH-33) Patricia Bouyer. From qualitative to quantitative analysis of timed systems. Mémoire d'habilitation, Université Paris 7, Paris, France, January 2009.

(TH-34) Ghassan Oreiby. Logiques temporelles pour le contrôle temporisé. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2008.

(TH-35) Myrto Arapinis. Sécurité des protocoles cryptographiques : décidabilité et résultats de réduction. Thèse de doctorat, Université Paris 12, Créteil, France, November 2008.

(TH-36) Elie Bursztein. Anticipation games. théorie des jeux appliqués à la sécurité réseau. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2008.

(TH-37) Arnaud Sangnier. Vérification de systèmes avec compteurs et pointeurs. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2008.

Notes de cours

(Nc-1) Sylvain Schmitz and Philippe Schnoebelen. Algorithmic aspects of WQO theory. Lecture Notes, August 2012.

(Nc-2) Nicolas Markey. Timed and hybrid automata. Course notes, Master Parisien de Recherche en Informatique, Paris, France, 2010.

(Nc-3) Nicolas Markey. Weighted automata : Model checking and games. Course notes, Master Parisien de Recherche en Informatique, Paris, France, 2008.

Rapports internes non publiés par ailleurs

(Ra-1) Fabrice Kordon, Alban Linard, Marco Becutti, Didier Buchs, Lukasz Fronc, Francis Hulin-Hubard, Fabrice Legond-Aubry, Niels Lohmann, Alexis Marechal, eMMANUEL Paviot-Adet, fRANCK Pommereau, César Rodríguez, Christian Rohr, Yann Thierry-Mieg, Haro Wimmel, and Karsten Wolf. Web report on the model checking contest @ petri net 2013, June 2013.

(Ra-2) Laurent Fribourg and Romain Soulat. Finite controlled invariants for sampled switched systems. Research Report LSV-13-09, Laboratoire Spécification et Vérification, ENS Cachan, France, April 2013. 27 pages.

(Ra-3) François Laroussinie and Nicolas Markey. Quantified CTL : expressiveness and complexity. Research Report LSV-13-07, Laboratoire Spécification et Vérification, ENS Cachan, France, April 2013. 41 pages.

(Ra-4) Youcheng Sun, Romain Soulat, Giuseppe Lipari, Étienne André, and Laurent Fribourg. Parametric schedulability analysis of fixed priority real-time distributed systems. Research Report LSV-13-03, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2013. 10 pages.

(Ra-5) Laurent Doyen and Alexander Rabinovich. Robot games. Research Report LSV-13-02, Laboratoire Spécification et Vérification, ENS Cachan, France, January 2013. 2 pages.

(Ra-6) Cristoph Haase, Sylvain Schmitz, and Philippe Schnoebelen. The power of priority channel systems. Research Report cs.LO/1207.4577v2, Computing Research Repository, January 2013. 32 pages.

(Ra-7) Rémy Chrétien. Trace equivalence of protocols for an unbounded number of sessions. Research Report LSV-12-22, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012. 30 pages.

(Ra-8) Gilles Feld, Laurent Fribourg, Denis Labrousse, Bertrand Revol, and Romain Soulat. Correct-by-design control of 5-level and 7-level power converters. Research Report LSV-12-25, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012. 8 pages.

(Ra-9) Laurent Fribourg and Romain Soulat. Controlled recurrent subspaces for sampled switched linear systems. Research Report LSV-12-24, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012. 11 pages.

(Ra-10) Steen Vester. Symmetric Nash equilibria. Research Report LSV-12-23, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012. 51 pages.

(Ra-11) Assalé Adjé and Jean Goubault-Larrecq. Concrete semantics of programs with non-deterministic and random inputs. Research Report cs.LO/1210.2605, Computing Research Repository, October 2012. 19 pages.

(Ra-12) Rohit Chadha and Michael Ummels. The complexity of quantitative information flow in recursive programs. Research Report LSV-12-15, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2012. 24 pages.

(Ra-13) Gilles Feld, Laurent Fribourg, Denis Labrousse, Bertrand Revol, and Romain Soulat. Numerical simulation and physical experimentation of a 5-level and 7-level power converter under a control designed by a formal method. Research Report LSV-12-16, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2012. 18 pages.

(Ra-14) Gilles Feld, Laurent Fribourg, Denis Labrousse, Stéphane Lefebvre, Bertrand Revol, and Romain Soulat. Control of multilevel power converters using formal methods. Research Report LSV-12-14, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2012. 14 pages.

(Ra-15) Romain Soulat. Scheduling with IMITATOR : Some case studies. Research Report LSV-12-05, Laboratoire Spécification et Vérification, ENS Cachan, France, March 2012. 13 pages.

(Ra-16) Benoît Barbot, Serge Haddad, and Claudine Picaronny. Importance sampling for model checking of time-bounded until. Research Report LSV-12-04, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2012. 14 pages.

(Ra-17) Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Modeling and verifying ad hoc routing protocols. Research Report LSV-11-24, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2011. 66 pages.

(Ra-18) Étienne Lozes and Jules Villard. Sharing contract-obedient endpoints. Research Report LSV-11-23, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2011. 42 pages.

(Ra-19) Dietmar Berwanger, Łukasz Kaiser, and Simon Leßenich. Imperfect recall and counter games. Research Report LSV-11-20, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2011.

(Ra-20) Jan Degrieck. *Réduction de graphes pour l'analyse de protocoles de routage sécurisés*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2011.

(Ra-21) Amit Kumar Dhar. *Counter Systems with Presburger-definable Reachability Sets : Decidability and Complexity*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2011.

(Ra-22) Daniel Pasailă. *Verifying equivalence properties of security protocols*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2011.

(Ra-23) Éric Florentin, Laurent Fribourg, Ulrich Kühne, Stéphane Lefebvre, and Christian Rey. COUPLET : Coupled electrothermal simulation. Research Report LSV-11-18, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2011. 32 pages.

(Ra-24) Benedikt Bollig, Paul Gastin, Benjamin Monmege, and Marc Zeitoun. Weighted expressions and DFS tree automata. Research Report LSV-11-08, Laboratoire Spécification et Vérification, ENS Cachan, France, April 2011. 32 pages.

(Ra-25) Laurent Fribourg and Ulrich Kühne. Parametric verification of hybrid automata using the inverse method. Research Report LSV-11-04, Laboratoire Spécification et Vérification, ENS Cachan, France, March 2011. 25 pages.

(Ra-26) Étienne André. Synthesizing parametric constraints on various case studies using IMITATOR II. Research Report LSV-10-21, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2010. 66 pages.

(Ra-27) Rémi Bonnet, Alain Finkel, Serge Haddad, and Fernando Rosa-Velardo. Comparing petri data nets and timed petri nets. Research Report LSV-10-23, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2010. 16 pages.

(Ra-28) Romain Soulat. On properties of the inverse method : Commutation of instanciation and full covering of the behavioral cartography. Research Report LSV-10-22, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2010. 14 pages.

(Ra-29) Étienne André. IMITATOR II user manual. Research Report LSV-10-20, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2010. 31 pages.

(Ra-30) Béatrice Bérard, Serge Haddad, Mathieu Sassolas, and Marc Zeitoun. Distributed synthesis with incomparable information. Research Report LSV-10-17, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2010. 20 pages.

(Ra-31) Adrien Boiret. *Grammaires Context-Free pour les arbres sans rang*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

(Ra-32) Aiswarya Cyriac. *Temporal Logics for Concurrent Recursive Programs*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

(Ra-33) Jérémie Dimino. *Sur les arbres de rang non borné avec données*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

(Ra-34) Benjamin Monmege. *Propriétés quantitatives des mots et des arbres – Applications aux langages XML*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

(Ra-35) César Rodríguez. *Implementation of a complete prefix unfolder for contextual nets*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

(Ra-36) Ocan Sankur. *Model-checking robuste des automates temporisés via les machines à canaux*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

(Ra-37) Guillaume Scerri. *Modélisation des clés de l'intrus*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2010.

(Ra-38) Romain Soulat. *Améliorations algorithmiques d'un moteur de model-checking et études de cas*. Rapport de Master, Master 2 Recherche Informatique Paris Sud 11, September 2010.

(Ra-39) Rémi Bonnet. *Well-structured Petri Nets extensions with data*. Rapport de Master, Master Computer Science, EPFL, Lausanne, Switzerland, March 2010.

(Ra-40) Jérémie Dimino. *Les systèmes à canaux non-fiables vus comme des transducteurs*. Rapport de stage de M1, Master Parisien de Recherche en Informatique, Paris, France, October 2009.

(Ra-41) Romain Brenguier. *Calcul des équilibres de Nash dans les jeux temporisés*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2009.

(Ra-42) Vincent Cheval. *Algorithme de décision de l'équivalence symbolique de systèmes de contraintes*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2009.

(Ra-43) Étienne André. Everything you always wanted to know about IMITATOR (but were afraid to ask). Research Report LSV-09-20, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2009. 11 pages.

(Ra-44) Béatrice Bérard, Serge Haddad, and Mathieu Sassolas. Verification on interrupt timed automata. Research Report LSV-09-16, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2009. 16 pages.

(Ra-45) Pierre-Cyrille Héam and Cyril Nicaud. Seed : an easy-to-use random generator of recursive data structures for testing. Research Report LSV-09-15, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2009. 16 pages.

(Ra-46) Étienne André, Emmanuelle Encrenaz, and Laurent Fribourg. Synthesizing parametric constraints on various case studies using IMITATOR. Research Report LSV-09-13, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2009. 18 pages.

(Ra-47) Jean Goubault-Larrecq. On a generalization of a result by Valk and Jantzen. Research Report LSV-09-09, Laboratoire Spécification et Vérification, ENS Cachan, France, May 2009. 18 pages.

(Ra-48) Sergiu Bursuc and Hubert Comon-Lundh. Protocols, insecurity decision and combination of equational theories. Research Report LSV-09-02, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2009. 43 pages.

(Ra-49) Ştefan Ciobâcă. *Verification of anonymity properties in e-voting protocols*. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, September 2008.

(Ra-50) Jean Goubault-Larrecq. A cone-theoretic Krein-Milman theorem. Research Report LSV-08-18, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2008. 8 pages.

(Ra-51) Alain Finkel and Jérôme Leroux. Presburger functions are piecewise linear. Research Report LSV-08-08, Laboratoire Spécification et Vérification, ENS Cachan, France, March 2008. 9 pages.

(Ra-52) Jules Villard, Étienne Lozes, and Ralf Treinen. A spatial equational logic for the applied pi-calculus. Research Report LSV-08-10, Laboratoire Spécification et Vérification, ENS Cachan, France, March 2008. 44 pages.

(Ra-53) Elie Bursztein. Network administrator and intruder strategies. Research Report LSV-08-02, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2008. 23 pages.

Rapports de contrats

(Rc-1) Sandie Balaguer, Thomas Chatain, and Stefan Haar. Concurrent semantics for timed distributed systems. Deliverable ImpRo D 4.1 (ANR-2010-BLAN-0317), March 2012.

(Rc-2) Radu Iosif, Peter Habermehl, Sebastien Labbe, Étienne Lozes, and Boris Yakobowski. Concurrent programs with simple data structures / sequential programs with composite data structures. Deliverable VERIDYC D 2 (ANR-09-SEGI-016), March 2012.

(Rc-3) S. Akshay, Béatrice Bérard, Patricia Bouyer, Stefan Haar, Serge Haddad, Claude Jard, Didier Lime, Nicolas Markey, Pierre-Alain Reynier, Ocan Sankur, and Yann Thierry-Mieg. Overview of robustness in timed systems. Deliverable ImpRo D 2.1 (ANR-2010-BLAN-0317), January 2012.

(Rc-4) Étienne André, Abdelrezzak Bara, Pirouz Bazargan-Sabet, Rémy Chevallier, Dominique Le Dû, Emmanuelle Encrenaz, Laurent Fribourg, and Patricia Renault. Compte-rendu de fin du projet ANR VALMEM, January 2011. 14 pages.

(Rc-5) Stéphanie Delaune. Algorithms for observational equivalence. Deliverable AVOTE 2.2, (ANR-07-SESU-002), January 2011. 118 pages.

(Rc-6) Steve Kremer. Results on case studies from literature. Deliverable AVOTE 4.2, (ANR-07-SESU-002), January 2011. 96 pages.

(Rc-7) Étienne André, Abdelrezzak Bara, Pirouz Bazargan-Sabet, Rémy Chevallier, Dominique Le Dû, Emmanuelle Encrenaz, Laurent Fribourg, and Patricia Renault. Experiments of prototype tools on case studies, comparison of obtained results and conclusion. Deliverables VALMEM 4.2 and 4.3, (ANR-06-ARFU-005), December 2010. 31 pages.

(Rc-8) Stéphanie Delaune and Steve Kremer. Formalising security properties in electronic voting protocols. Deliverable AVOTE 1.2, (ANR-07-SESU-002), April 2010. 17 pages.

(Rc-9) Véronique Cortier, Steve Kremer, and Pascal Lafourcade. Computational soundness of static equivalence. Deliverable AVOTE 3.1, (ANR-07-SESU-002), March 2010. 106 pages.

(Rc-10) Nicolas Markey, Shuhao Li, Jean-François Raskin, and Mariëlle Stoelinga. Synthesizing controllers with bounded resources. Deliverable QUASIMODO 3.4 (ICT-FP7-STREP-214755), January 2010.

(Rc-11) LIAFA, CRIL, EDF, LSV, and Verimag. Projet RNTL Averiles – fourniture f2.2 : Algorithmes de vérification – rapport final, November 2009. 25 pages.

(Rc-12) Ştefan Ciobâcă and Véronique Cortier. Algorithmes pour l'équivalence statique. Deliverable AVOTE 2.1 (ANR-07-SESU-002), September 2009. 17 pages.

(Rc-13) François Laroussinie, Frits Vaandrager, and Martin Neuhäußer. Extended timed automata for scheduling. Deliverable QUASIMODO 3.5 (ICT-FP7-STREP-214755), July 2009.

(Rc-14) Nicolas Markey, Jasper Berendsen, Alexandre David, Tingting Han, Holger Hermanns, Kim G. Larsen, and Martin Neuhäußer. Symbolic data structures and analysis of models with multiple quantitative aspects. Deliverable QUASIMODO 2.2 (ICT-FP7-STREP-214755), July 2009.

(Rc-15) Patricia Bouyer, François Laroussinie, Didier Lime, and Nicolas Markey. Synthesis of timed controllers. Deliverable DOTS 1.2a (ANR-06-SETI-003), March 2009.

(Rc-16) Thomas Chatain, Paul Gastin, Anca Muscholl, Nathalie Sznajder, Igor Walukiewicz, and Marc Zeitoun. Distributed control for restricted specifications. Deliverable DOTS 2.2 (ANR-06-SETI-003), March 2009.

(Rc-17) Patricia Bouyer, Joost-Pieter Katoen, Rom Langerak, François Laroussinie, Nicolas Markey, and Jean-François Raskin. Transfer of correctness from models to implementation. Deliverable QUASIMODO 3.1 (ICT-FP7-STREP-214755), January 2009.

(Rc-18) Stéphanie Delaune and Steve Kremer. Spécificités des protocoles de vote électronique. Deliverable AVOTE 1.1 (ANR-07-SESU-002), January 2009. 8 pages.

(Rc-19) Benedikt Bollig, Patricia Bouyer, Franck Cassez, Thomas Chatain, Paul Gastin, Serge Haddad, and Claude Jard. Model for distributed timed systems. Deliverable DOTS 3.1 (ANR-06-SETI-003), September 2008.

(Rc-20) Franck Cassez, François Laroussinie, Didier Lime, and Nicolas Markey. Quantitative objectives in timed games. Deliverable DOTS 1.1 (ANR-06-SETI-003), September 2008.

(Rc-21) François Laroussinie et al. Projet dots (anr-06-seti-003) : Rapport à 18 mois, September 2008. 5 pages.

(Rc-22) François Laroussinie et al. Projet dots (anr-06-seti-003) : Rapport à 12 mois, March 2008. 6 pages.

Réalisations informatiques

(Lo-1) Romain Brenguier. PRALINE, 2013.

(Lo-2) Ocan Sankur. Shrinktech, 2013.

(Lo-3) Julien Olivain, Jean Goubault-Larrecq, Hedi Benzina, Baptiste Gourdin, and Romdhane Ben Younès. ORCHIDS, 2011.

(Lo-4) Étienne André, Romain Soulat, and Ulrich Kühne. Imitator II, March 2011.

(Lo-5) César Rodríguez and Stefan Schwoon. Cunf, February 2011.

(Lo-6) Jules Villard and Étienne Lozes. Heap-hop, February 2011.

(Lo-7) Ştefan Ciobâcă. KiSs, 2010.

(Lo-8) Matteo Bortolozzo, Matteo Centenaro, Riccardo Focardi, and Graham Steel. Tookan, December 2010.

(Lo-9) Étienne André. Imitator, August 2009.

(Lo-10) Étienne André. Imprator, April 2009.

(Lo-11) Jean Goubault-Larrecq. HimML : **H**imML **is** a **m**ap-oriented **ML**, December 2008.

(Lo-12) Elie Bursztein. Netanalyzer v0.7.5, January 2008. Written in C and Perl (about 25000 lines).

(Lo-13) Jean Goubault-Larrecq. The h1 tool suite, January 2008.

agence d'évaluation de la recherche et de l'enseignement supérieur

Annexe 7 :
Liste des thèses

Liste des thèses de doctorat

Thèses soutenues entre le 1er janvier 2008 et le 30 juin 2013

- Ocan SANKUR. *Robustness in Timed Automata : Analysis, Synthesis, Implementation*. Thèse de doctorat soutenue le 24 mai 2013. (TH-1).
- Rémi BONNET. *Theory of well-structured transition systems and extended vector-addition systems*. Thèse de doctorat soutenue le 22 janvier 2013. (TH-2).
- Hedi BENZINA. *Enforcing virtualized systems security*. Thèse de doctorat soutenue le 17 décembre 2012. (TH-4).
- Sandie BALAGUER. *La concurrence dans les systèmes distribués temps-réel*. Thèse de doctorat soutenue le 13 décembre 2012. (TH-3).
- Vincent CHEVAL. *Automatic verification of cryptographic protocols : privacy-type properties*. Thèse de doctorat soutenue le 03 décembre 2012. (TH-5).
- Romain BRENGUIER. *Équilibres de Nash dans les jeux concurrents – Application aux jeux temporisés*. Thèse de doctorat soutenue le 29 novembre 2012. (TH-6).
- Hilal DJAFRI. *Approches numériques et statistiques pour le model checking des processus stochastiques*. Thèse de doctorat soutenue le 19 juin 2012. (TH-8).
- Mathilde ARNAUD. *Formal verification of secured routing protocols*. Thèse de doctorat soutenue le 13 décembre 2011. (TH-10).
- Ştefan CIOBÂCĂ. *Automated verification of security protocols with appplications to electronic voting*. Thèse de doctorat soutenue le 09 décembre 2011. (TH-11).
- Pierre CHAMBARD. *Du problème de sous-mot de Post et de la complexité des canaux non fiables*. Thèse de doctorat soutenue le 29 septembre 2011. (TH-13).
- Alban GALLAND. *Distributed data management with access control*. Thèse de doctorat soutenue le 28 septembre 2011. (TH-15).
- Arnaud DA COSTA LOPES. *Propriétés de jeux multi-agents*. Thèse de doctorat soutenue le 20 septembre 2011. (TH-14).
- Jules VILLARD. *Heaps and hops*. Thèse de doctorat soutenue le 18 février 2011. (TH-21).
- Pierre BOURHIS. *On the dynamics of active documents for distributed data management*. Thèse de doctorat soutenue le 11 février 2011. (TH-20).

- Thomas Place. *Decidable characterizations for tree logics*. Thèse de doctorat soutenue le 10 décembre 2010. (TH-24).
- Étienne André. *An inverse method for the synthesis of timing parameters in concurrent systems*. Thèse de doctorat soutenue le 08 décembre 2010. (TH-22).
- Camille Vacher. *Automates à contraintes globales pour la vérification de propriétés de sécurité*. Thèse de doctorat soutenue le 07 décembre 2010. (TH-25).
- Diego Figueira. *On decidable automata on data words and data trees in relation to satisfiability of LTL and XPath*. Thèse de doctorat soutenue le 06 décembre 2010. (TH-23).
- S. Akshay. *Spécification et vérification pour des systèmes distribués et temporisés*. Thèse de doctorat soutenue le 02 juillet 2010. (TH-26).
- Jean-Loup Carré. *Analyse statique de programmes multi-thread pour l'embarqué*. Thèse de doctorat soutenue le 02 juillet 2010. (TH-27).
- Antoine Mercier. *Contributions à l'analyse automatique des protocoles cryptographiques en présence de propriétés algébriques : protocoles de groupe, équivalence statique*. Thèse de doctorat soutenue le 04 décembre 2009. (TH-29).
- Sergiu Bursuc. *Contraintes de déductibilité dans une algèbre quotient : réduction de modèles et applications à la sécurité*. Thèse de doctorat soutenue le 01 décembre 2009. (TH-28).
- Nathalie Sznajder. *Synthèse de systèmes distribués ouverts*. Thèse de doctorat soutenue le 12 novembre 2009. (TH-31).
- Florent Bouchy. *Logiques et modèles pour la vérification de systèmes infinis*. Thèse de doctorat soutenue le 10 novembre 2009. (TH-30).
- Najla Chamseddine. *Analyse quantitative parametrée d'automates temporisés probabilistes*. Thèse de doctorat soutenue le 27 octobre 2009. (TH-32).
- Ghassan Oreiby. *Logiques temporelles pour le contrôle temporisé*. Thèse de doctorat soutenue le 08 décembre 2008. (TH-34).
- Elie Bursztein. *Anticipation games. Théorie des jeux appliqués à la sécurité réseau*. Thèse de doctorat soutenue le 26 novembre 2008. (TH-36).
- Arnaud Sangnier. *Vérification de systèmes avec compteurs et pointeurs*. Thèse de doctorat soutenue le 21 novembre 2008. (TH-37).

Liste des thèses en cours au 1er juillet 2013

- Émilien Antoine. *Partage d'informations dans un réseau social*. Thèse de doctorat commencée en septembre 2010.
- Benoît Barbot. *Accélérations pour le model checking statistique*. Thèse de doctorat commencée en septembre 2011.
- Rémi Brochenin. *Separation Logic : Expressiveness, Complexity, Temporal Extension*. Thèse de doctorat commencée en septembre 2007.
- Rémy Chrétien. *Vérification de propriétés d'anonymat pour les protocoles sécurisés*. Thèse de doctorat commencée en octobre 2012.
- Aiswarya Cyriac. *Logique temporelle pour les systèmes récursifs et concurrents*. Thèse de doctorat commencée en octobre 2010.
- Nadime Francis. *Graph data processing*. Thèse de doctorat commencée en septembre 2011.
- Prateek Karandikar. *Post embedding problems and algorithmic verification for infinite state systems*. Thèse de doctorat commencée en septembre 2012.
- Wojtech Kazana. *Query evaluation with constant delay*. Thèse de doctorat commencée en mars 2010.

- Robert KÜNNEMANN. *Foundations for analysing security APIs*. Thèse de doctorat commencée en septembre 2010.
- Benjamin MONMEGE. *Vérification de propriétés quantitatives – Applications aux requêtes pour documents XML*. Thèse de doctorat commencée en septembre 2010.
- Hernan PONCE DE LEON. *Test de systèmes concurrents à l'aide de structures d'évènements*. Thèse de doctorat commencée en septembre 2011.
- Julien REICHERT. *Games with counters : decidability and algorithms*. Thèse de doctorat commencée en septembre 2011.
- César RODRÍGUEZ. *Contextual Petri nets and their applications*. Thèse de doctorat commencée en septembre 2010.
- Guillaume SCERRI. *Preuves abstraites de protocoles cryptographiques concrets*. Thèse de doctorat commencée en septembre 2011.
- Mahsa SHIRMOHAMMADI. *Quantitative verification for reactive systems*. Thèse de doctorat commencée en octobre 2010.
- Romain SOULAT. *Synthèse de contrôle pour les systèmes hybrides*. Thèse de doctorat commencée en octobre 2010.
- Marie VAN DEN BOGAARD. *Information-flow patterns and cores*. Thèse de doctorat commencée en septembre 2012.

Liste des thèses d'habilitation

- Étienne LOZES. *Separation logic : Expressiveness and copyless message-passing*. Thèse d'habilitation soutenue le 03/07/2012. (TH-7).
- Laurent DOYEN. *Games and automata : From boolean to quantitative verification*. Thèse d'habilitation soutenue le 13/03/2012. (TH-9).
- Florent JACQUEMARD. *Extended tree automata for the verification of infinite state systems*. Thèse d'habilitation soutenue le 10/11/2011. (TH-12).
- Nicolas MARKEY. *Verification of embedded systems – algorithms and complexity*. Thèse d'habilitation soutenue le 08/04/2011. (TH-16).
- Stéphanie DELAUNE. *Verification of security protocols : from confidentiality to privacy*. Thèse d'habilitation soutenue le 18/03/2011. (TH-17).
- Steve KREMER. *Modelling and analyzing security protocols in cryptographic process calculi*. Thèse d'habilitation soutenue le 17/03/2011. (TH-18).
- Graham STEEL. *Formal analysis of security APIs*. Thèse d'habilitation soutenue le 17/03/2011. (TH-19).
- Patricia BOUYER. *From qualitative to quantitative analysis of timed systems*. Thèse d'habilitation soutenue le 12/01/2009. (TH-33).